奇安信
新一代网络安全领军者

零信任安全 新身份边界



深度解读

零信任身份安全

第 II 辑

奇安信身份安全实验室

VISIT…

LANZAROTE Caliente.com

深度解读
零信任身份安全
专辑 II

奇安信身份安全实验室

深度解读：

1. 零信任安全 新身份边界
2. 零信任架构在关键信息基础设施安全保护中的应用研究
3. 零信任迁移方法论

行业研读：

1. BeyondProd：一种新的云原生安全方法
2. 谷歌基础架构安全设计概述——谷歌云白皮书
3. NIST 标准《零信任架构》Draft 1 全文
4. NIST 标准《零信任架构》草案第 1、2 版全文对比与解读
5. NIST NCCoE 指南《实现零信任架构》（草案)

奇安信身份安全实验室出品

前言

奇安信身份安全实验室，奇安信集团下属专注“零信任身份安全架构”研究的专业实验室，是业界首部零信任安全技术图书《零信任网络：在不可信网络中构建安全系统》译者。该团队以“零信任安全，新身份边界”为技术思想，推出“以身份为基石、业务安全访问、持续信任评估、动态访问控制”为核心的奇安信零信任身份安全解决方案。该团队结合行业现状，大力投入对零信任安全架构的研究和产品标准化，积极推动“零信任身份安全架构”在业界的落地实践，其方案已经在部委、央企、金融等行业进行广泛落地实施，得到市场、业界的高度认可。

本文集为奇安信身份安全实验室“深度解读零信任身份安全”系列第二辑，由以下 3 部分组成：谷歌云安全论文系列译文 2 篇；美国国家标准技术研究所（NIST）《零信任架构》草案译文及解读 3 篇；以及结合国内外行业实际情况，对零信任安全的理念、技术、实践方案的原创作品 3 篇。在此仅供国内业界各位同仁参考、交流。论文及草案原文来自于谷歌及 NIST 官网，如有侵权，请联系删除。同时，文章中难免出现错误或不妥之处，敬请谅解并欢迎批评指正。联系邮箱：zhangliting@qianxin.com。

关于零信任安全的更多资讯和最新研究解读，欢迎关注《深度解读零信任身份安全专栏》，以及微信公众号“零信任安全社区”。





奇安信身份安全实验室出品

目录

前言......3
目录......4
零信任安全 新身份边界......5
零信任架构在关键信息基础设施安全保护中的应用研究......10
零信任迁移方法论......18
BeyondProd：一种新的云原生安全方法......20
谷歌基础架构安全设计概述——谷歌云白皮书......32
NIST 标准《零信任架构》草案 1 全文......46
NIST 标准《零信任架构》草案第 1、2 版全文对比与解读......79
NIST NCCoE 指南《实现零信任架构》（草案）......128

奇安信身份安全实验室出品

零信任安全 新身份边界

2017年，身份安全发生了两件大事情。其一，RSAC2017上，UnifyID一举夺得创新沙盒的的冠军。UnifyID可以从IoT设备中收集传感器数据，依赖100多个同步的因素，并结合机器学习，为用户构建“绝对身份”，准确率可达99.999%。UnifyID在向外界传达一个信号，任何静态的、单一维度的认证因子，都无法保证用户身份的合法性，必须结合多维度数据，对用户身份展开持续的验证。

其二，谷歌宣布基于零信任理念构建的新一代网络安全架构——BeyondCorp成功完成，大部分应用已经成功迁移至该架构上。自此，零信任大热了起来。

到2018年的时候，零信任就已经非常火了，网络巨头思科不惜斥资23.8亿元收购身份安全厂商DUO。并且那一年，奇安信又提出了“安全从0开始”，把国内零信任的这股风也吹了起来。结合国内的政企客户实践，奇安信赋予了零信任架构四大关键能力：以身份为基石、业务安全访问、持续信任评估和动态访问控制，最终在访问主体和访问客体之间建立一种动态的信任关系，并基于信任关系赋予动态的访问权限。

再到2019年，RSAC上主打零信任的厂商就逐渐开始增多，大致有39家。而到了今年，RSAC上打着零信任标签的厂商就已经有91家之多，是去年的两倍以上，零信任也因此成为了RSAC2020热度增长最快的热词之一。

那么，究竟什么是零信任？

零信任（或零信任网络、零信任架构、零信任模型、零信任安全）这个概念最早是由John Kindervag于2010年正式提出的，他当时是Forrester的分析师。John非常敏锐地发现传统的基于边界的网络安全架构存在缺陷，通常被认为“可信”的内部网络充满着威胁，“信任”被过度滥用，并指出“信任是安全的致命弱点”。因此，John创造出了零信任（Zero Trust）这个概念。“从来不信任，始终在校验”（Never Trust，Always Verify）是零信任的核心思想。也就是说，默认情况下不应该信任网络内部和外部的任何人、设备、系统和应用，而是应该基于认证和授权重构访问控制的信任基础，并且这种授权和信任不是静态的，而是需要基于对访问主体的风险度量进行动态调整。

传统的网络安全架构是基于网络边界防护的安全架构。企业构建网络安全体系时，首先把网络划分为外网、内网、DMZ区等不同的安全区域，然后在网络边界上通过部署防火墙、WAF、IPS等网络安全技术手段进行重重防护，构筑企业业务的数字护城河。这种网络安全架构假设或默认了内网比外网更安全，在某种程度上预设了对内网中的人、设备、系统和应用的信任，从而忽视内网安全措施的加强。美国Verizon公司《数据泄露调查报告》曾指出，造成企业数据泄露的原因主要有两类，一是外部攻击，二是内部威胁。随着网络攻防技术的发展，新型的网络攻击手段层出不穷，攻击者面对层层设防的网络边界，往往会放弃代价高昂的强攻手段，而是针对企业内部网络中的计算机，采用钓鱼邮件、水坑攻击等方法渗透到企业网络内部，轻松绕过网络边界安全防护措施。由于人们往往认为内网是可信任的，所以攻击者一旦突破企业的网络安全边界进入内网，常常会如入无人之境。此外，企业员工、外包人员等内部用户通常拥有特定业务和数据的合法访问权限，一旦出现凭证丢失、权限滥用或恶意非授权访问等问题，同样会导致

© 2020 奇安信集团 保留所有权利

企业的数据泄漏。

基于这样的认知，零信任安全针对传统边界安全架构思想进行了重新评估和审视，并对安全架构思路给出了新的建议，《零信任网络》作者使用如下五句话对“零信任“这个概念进行了抽象概括：

- 应该假设网络自始至终充满威胁；
- 网络中的威胁既包括外部威胁，也包括内部威胁；
- 不能仅仅依靠网络位置来评估信任；
- 所有用户、设备和网络流量都应该被认证、授权和加密；
- 访问控制策略应该是动态的，并基于尽可能多的数据源进行计算和评估。

零信任对网络安全架构进行了范式上的颠覆，引导安全体系架构从基于网络走向基于身份，其本质诉求是以身份为基石进行细粒度的自适应访问控制。零信任所依赖的身份认证与访问控制能力通常由身份与访问管理系统（IAM）提供，现代身份管理技术是零信任安全的技术根基，因此，从技术方案层面来看，零信任安全是借助现代身份管理技术实现对人、设备、系统和应用的全面、动态、智能的访问控制。

零信任架构的技术实践具有以下特点：

1) 以身份为基石：基于身份而非网络位置来构建访问控制体系，首先需要为网络中的人和设备赋予数字身份，将身份化的人、设备和应用进行运行时组合构建访问主体，并为访问主体设定其所需的最小权限。在零信任架构中，根据一定的访问上下文，访问主体可以是人、设备和应用等实体数字身份的动态组合，在《零信任网络》一书中，将这种组合称为网络代理。网络代理指在网络请求中用于描述请求发起者的信息集合，一般包括用户、应用程序和设备共三类实体信息，用户、应用程序和设备信息是访问请求密不可分的上下文。

2) 业务安全访问：零信任架构关注业务保护面的构建，通过业务保护面实现对资源的保护，在零信任架构中，应用、服务、接口、数据都可以视作业务资源。通过构建保护面实现对暴露面的收缩，要求所有业务默认隐藏，根据授权结果进行最小程度的开放，所有的业务访问请求都应该进行全流量加密和强制授权，业务安全访问相关机制需要尽可能工作在应用协议层。

3) 持续信任评估：持续信任评估是零信任体系从零开始构建信任的关键手段，通过信任评估模型和算法，实现基于身份的信任评估能力，同时需要对访问的上下文环境进行风险判定，对访问请求进行异常行为识别，并对信任评估结果进行调整。前文提到，在零信任架构中，访问主体是人、设备和应用程序三者结合构成的网络代理，因此在基础的身份信任的基础上，还需要评估主体信任，主体信任是对身份信任在当前访问上下文中的动态调整，和认证强度、风险状态和环境因素等相关，身份信任相对稳定，而主体信任和网络代理一样，具有短时性特征，是一种动态信任，基于主体的信任等级进行动态访问控制也是零

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

信任的本质所在。

4) 动态访问控制：动态访问控制是零信任架构的安全闭环能力的重要体现。建议通过 RBAC 和 ABAC 的组合授权实现灵活的访问控制基线，基于信任等级实现分级的业务访问，同时，当访问上下文和环境存在风险时，需要对访问权限进行实时干预并评估是否对访问主体的信任进行降级。

客观地说，John Kindervag 提出零信任架构的前几年，这一理念并没有获得网络安全行业的普遍关注，只是在一些社区有着小范围的讨论和实践。究其原因，笔者认为主要有三个方面。第一，当时的网络安全威胁形式不如当前这么严峻，高级的攻击技战术还不像现在这么普及，只是掌握在非常少数的攻击者手中，APT 攻击、网络杀伤链（Cyber Kill Chain）这些概念还没有出现，传统的网络边界安全架构能够应对主流的网络安全威胁，外部驱动力不足。第二，当时的 IT 技术架构尚未出现大规模的变革，传统的数据中心、传统的网络架构仍然是主流的 IT 基础设施，云计算、大数据技术、BYOD 等新技术还没有得到普及。应用和数据的控制权基本完全掌握在企业的 IT 部门手中，很容易划分网络安全域，网络安全边界非常清晰，企业 IT 安全部门改变安全架构的内在驱动力不足。第三，零信任不是简单地在原有安全体系基础上叠加新的安全产品或技术方案，而是对传统基于网络边界的安全架构的彻底颠覆，是安全基础架构层面的变革，涉及的不仅是技术问题，还涉及安全策略问题、安全管理问题，甚至涉及企业内部网络安全相关权责及组织结构的变革，这种变革付出的代价是比较大的，当内、外部的驱动力不足时，企业从安全投入和产出回报的角度考虑，变革的动力自然会降低。

2015 年前后，情况发生了明显的变化。层出不穷的高级威胁和内部威胁，以及监管机构对企业网络安全的监督力度逐渐加强，使得零信任架构变革的外部驱动力越来越强。随着企业数字化转型的逐渐深入，以云计算、微服务、大数据、移动计算为代表的新一代信息化建设浪潮愈演愈烈，IT 基础设施的技术架构发生了剧烈的变革，导致传统的内外网络边界变得模糊，很难找到物理上的网络安全边界，企业自然无法基于传统的边界安全架构理念构筑安全基础设施。安全架构如果不能随需应变，自然会成为木桶最短的那块木板，零信任架构变革的内生驱动力也在持续加强。

2017 年，Google 对外宣布其基于零信任理念构建的新一代企业网络安全架构——BeyondCorp 项目成功完成，为零信任安全在大型、新型企业网络的实践提供了参考架构。这一最佳实践成为零信任理念的助推剂，各大安全厂商、分析机构、大型企业快速跟进，对零信任的推广和宣传也持续升温，零信任俨然成为网络安全界的新宠。

Google BeyondCorp 项目的目标是摒弃企业特权网络并开创一种全新的访问模式。在这种全新的无特权网络访问模式下，访问只依赖于设备和用户凭证，而与用户所处的网络位置无关。用户无论是在公司“内网”、家庭网络、酒店还是咖啡店的公共网络，所有对企业资源的访问都要基于设备状态和用户凭证进行认证、授权和加密。这种新的访问模式可以针对不同的企业资源进行细粒度的访问控制，所有 Google 员工都可以从任何网络成功发起访问，无需通过传统的 VPN 连接进入特权网络，除了可能存在延迟差异外，对企业资源的本地和远程访问用户体验基本一致。BeyondCorp 项目的目标是“让所有 Google 员工从不受信任的网络中不接入 VPN 就能顺利工作”。尽管听起来像是要解决远程访问的接入安全问题，BeyondCorp 本质上是基于零信任架构理念，抛弃了对本

© 2020 奇安信集团 保留所有权利

地内网的信任，使用全新的安全架构取代基于网络边界构筑安全体系的传统做法。抛弃安全边界的概念后，BeyondCorp 构建了中心化的认证、授权和动态访问控制系统，着眼于保护 Google 的业务应用和数据，从而真正彻底改变了企业的安全体系，成为零信任安全架构的最佳实践。

当然，任何一种新生事物都难免受到人们的质疑，零信任架构也不例外。在过去一年多时间推广和实践零信任的过程中，我们遇到的最多的质疑是：零信任听起来并没有什么新技术，是不是“新瓶装旧酒”？的确，零信任是一种全新的安全架构，但其核心组件基于身份与访问管理技术、终端设备环境风险评估技术、基于属性的访问控制模型、基于机器学习的身份分析技术等构建，听上去并没有太激动人心。并且，零信任的最佳实践反倒是推荐使用现有的成熟技术，根据具体的应用场景，按照全新的逻辑进行组合，就能起到完全不同的安全效果。

我们认为零信任的创新和价值恰恰不在于具体的组件技术本身，而在于架构理念和安全逻辑层面。零信任架构与传统的边界安全架构和传统的安全防护理念最大的不同之处在于以下几点。第一，在网络安全边界瓦解、攻击面难以穷尽的情形下，与传统的安全理念不同，零信任架构引导人们更加关注“保护面”而不是“攻击面”。首先识别需要重点保护的资源对象，然后穷举分析该资源对象的访问路径，最后采用恰当的技术手段做好每条路径的访问控制措施。第二，零信任架构认为网络是不可信任的，因此不再寄希望于在传统的网络层面增强防护措施，而是把防护措施建立在应用层面，构建从访问主体到客体之间端到端的、最小授权的业务应用动态访问控制机制，极大地收缩了攻击面；采用智能身份分析技术，提升了内外部攻击和身份欺诈的发现和响应能力。第三，零信任架构在实践机制上拥抱灰度哲学，以安全与易用平衡的持续认证改进固化的一次性强认证，以基于风险和信任持续度量的动态授权替代简单的二值判定静态授权，以开放智能的身份治理优化封闭僵化的身份管理。因此，灰度哲学是零信任安全的内生逻辑，也是零信任安全实践的指导原则。

需要指出的是，零信任并不是解决一切网络安全问题的灵丹妙药。网络安全是动态的，不是静态的，威胁格局始终在发生变化，网络安全领域没有“银弹”，零信任当然也不是这颗“银弹”。零信任架构自身也有其局限性。首先，零信任架构相关技术方案的部署实施成本比较高，需要仔细权衡安全投入的价值回报。其次，在攻击者眼中，零信任安全设施的价值非常高，一旦攻陷就可以控制整个网络和应用，所以零信任安全设施更容易成为攻击者的目标。第三，零信任安全设施的软硬件实现自身同样可能存在软硬件漏洞，从而成为攻击者利用的对象。以上这些局限性，都是我们在部署实施零信任架构时需要重点考虑的问题。

零信任是一种全新的安全理念，它并不是严格定义的技术术语，这个概念的内涵和外延仍然处于变化之中。我们也不认为本书是一本零信任的教科书或者“圣经”，本书作者为我们揭示了零信任的基本概念和体系架构，并且通过实例介绍了如何利用现有的技术逐步构建一个零信任网络。我们希望通过翻译成中文的方式，可以把零信任的理念系统完整地介绍给国内的网络安全业界同仁，供大家讨论、实践和探索，甚至批判。希望能够通过这种方式，让更多的人理解和实践零信任理念，推动企业网络安全架构的转型和变革，为云计算和大数据时代的业务应用及数据保驾护航，并在此过程中不断丰富甚至修正零信任的内涵和外延，让零信任架构更加成熟，更加实用。

© 2020 奇安信集团 保留所有权利

本书的译者团队来自奇安信集团身份安全实验室。他们既是零信任架构理念的倡导者，也是零信任架构技术方案在国内大型企业落地部署的实践者。在实践过程中，他们对于零信任架构有了更加深刻的理解和认识，特别是针对国内大型部委和企业的 IT 技术架构，零信任架构落地部署需要更多特殊的安全视角和权衡。因此，本书关于零信任架构的某些技术实践细节并不一定完全适用于国内的 IT 技术环境，需要根据实际情况加以修正和补充。幸运的是，零信任架构本就是一个抽象的、开放的、不断发展中的安全框架，对零信任架构的内涵和外延有不同的理解和认知无伤大雅。但是，为了尽可能准确、系统、完整地介绍本书作者对零信任的认知和实践，我们在繁忙的工作之余通读了本书英文原作，在忠于原著的基础上尽最大努力将其翻译成通俗易懂的中文。即便如此，碍于技术理解和英文写作的水平有限，本书在翻译过程中难免有疏漏和谬误之处，也欢迎读者朋友们批评指正。

（文章首发：图书《零信任网络：在不可信网络中构建安全系统》译者序，内容有部分修订）

奇安信身份安全实验室出品

零信任架构在关键信息基础设施安全保护中的应用研究

【摘要】

关键信息基础设施作为经济社会运行的神经中枢，是网络安全保护的重中之重。数字化转型浪潮下，关键信息基础设施面临前所未有的安全挑战，安全架构急需革新，零信任架构应运而生。本文论述了基于零信任架构的安全解决方案，指出零信任架构的“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四大关键能力，为关键信息基础设施保驾护航。

【关键词】

网络安全；动态访问控制；信任评估；关键信息基础设施安全

1. 引言

随着《中华人民共和国网络安全法》,《国家网络空间安全战略》、《网络安全等级保护制度2.0》、《中华人民共和国密码法》等一系列政策法规出台，国家网络安全的战略及法律法规标准框架不断细化、完善和延伸。[1]

《网络安全法》第三章“网络运行安全”，对关键信息基础设施安全保护的基本要求、部门分工以及主体责任等问题作了基本法层面的总体制度安排，并规定关键信息基础设施的具体范围和安全保护办法应由国务院制定。以此为规范依据，国家互联网办公室公布了《关键信息基础设施安全保护条例》征求意见稿，明确关键信息基础设施安全保护的核心地位。

关键信息基础设施作为经济社会运行的神经中枢，会对国计民生、社会运行，甚至国家安全产生重大的影响。随着信息技术的发展，关键信息基础设施加速与云计算、大数据、物联网、移动计算等新技术进行结合，正全方位进入信息化、数字化，为各行业带来创新发展和新的活力；同时，各行业产业模式的数字化转型与升级，孕育了关键信息基础设施互联互通的发展趋势，通过互联互通实现数据共享协同，提高生产力，提升创新能力。

新技术的采用让关键信息基础设施变得越来越复杂，关键信息基础设施的互联互通也导致了更多的网络攻击面，在当前的网络安全态势下，针对关键信息基础设施的新型攻击技术手段层出不穷，网络安全事件时有发生，同时，非授权访问、人员犯错、有意的数据窃取等内部威胁也层出不穷，关键信息基础设施面临前所未有的安全挑战。

[1] 奇安信韩永刚：内生安全助力关键信息基础设施保护 – 中国青年网 [EB/OL].(2019-10-30)[2019-11-05]. http://d.youth.cn/shrgch/201910/t20191030_12106997.htm

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

2. 零信任架构出现的背景

面对如此严峻的安全挑战，业界的安全意识不可谓不到位，安全投入不可谓不高，然而，安全效果却不尽如人意，安全事件层出不穷，传统安全架构失效背后的根源是什么呢？安全的根本在应对风险，而风险与“漏洞”息息相关，是什么“漏洞”导致传统安全架构失效呢？答案是信任。传统的基于边界的网络安全架构某种程度上假设或默认了内网的人和设备是值得信任的，认为安全就是构筑企业的数字护城河，通过防火墙、WAF、IPS等边界安全产品及方案对企业网络边界进行重重防护就足够了。但是，安全是相对的，假设系统一定有未被发现的漏洞、假设一定有已发现但仍未修补的漏洞、假设系统已经被渗透、假设内部人员不可靠，这就需要全新的网络安全架构来应对现代复杂的关键信息基础设施所面临的问题。零信任架构正是在这种背景下应运而生，是安全思维和安全架构进化的必然。

在《零信任网络》一书中，埃文·吉尔曼（Evan Gilman）和道格·巴斯(Doug Barth)将零信任架构建立在如下五个基本假定之上：

- 网络无时无刻不处于危险的环境中。
- 网络中自始至终存在外部或内部威胁。
- 网络的位置不足以决定网络的可信程度。
- 所有的设备、用户和网络流量都应当经过认证和授权。
- 安全策略必须是动态的，并基于尽可能多的数据源计算而来。[2]

美国国家标准技术研究院（NIST）在近期发布的《零信任架构》中指出，零信任架构是一种网络/数据安全的端到端方法，关注身份、凭证、访问管理、运营、终端、主机环境和互联的基础设施，认为零信任是一种关注数据保护的架构方法。[3]NIST 认为传统安全方案只关注边界防护，对授权用户开放了过多的访问权限。零信任架构的首要目标就是基于身份进行细粒度的访问控制，以便应对越来越严峻的越权横向移动风险。

基于如上观点，NIST 对零信任架构定义如下：零信任架构提供一系列概念、理念、组件及其交互关系，以便消除针对信息系统和服务进行精准访问判定所存在的不确定性。

3. 基于零信任架构的安全解决方案

零信任架构的本质是在访问主体和客体之间构建以身份为基石的动态可信访问控制体系，通过以身份为基石、业务安全访问、持续信任评估和动态访问控制的关键能力，基于对网络所有参与实体的数字身份，对默认不可信的所有访问请求进行加密、认证和强制授权，汇聚关联各种数据源进行持续信任评估，并根据信任的程度动态对权限进行调整，最终在访问主体和访问客体之间建立一种动态的信任关系，如图 1 所示。

---

[2] 埃文·吉尔曼，道格·巴斯. 零信任网络 在不可信网络中构建安全系统[M].北京:人民邮电出版社,2019:1~2.
[3] 网络安全架构：零信任架构正在标准化:安全内参 [EB/OL].(2019-09-28)[2019-11-05]. https://www.secrss.com/articles/14045.

奇安信集团内部资料 (watermark)



图 1 零信任架构的核心能力

零信任架构下，访问客体是核心保护的资源，针对被保护资源构建保护面，资源包括但不限于业务应用、服务接口、操作功能和数据等关键信息基础设施。访问主体包括人员、设备、应用和系统等身份化之后的数字实体，在一定的访问上下文中，这些实体还可以进行组合绑定，进一步对主体进行明确和限定。

3.1 零信任架构的关键能力

（1）以身份为基石

基于身份而非网络位置来构建访问控制体系，首先需要为网络中的人和设备赋予数字身份，将身份化的人、设备和应用进行运行时组合构建访问主体，并为访问主体设定其所需的最小权限。在零信任架构中，根据一定的访问上下文，访问主体可以是人、设备和应用等实体数字身份的动态组合，在《零信任网络》一书中，将这种组合称为网络代理。网络代理指在网络请求中用于描述请求发起者的信息集合，一般包括用户、应用程序和设备共三类实体信息，用户、应用程序和设备信息是访问请求密不可分的上下文。[4]

（2）业务安全访问

零信任架构关注业务保护面的构建，通过业务保护面实现对资源的保护，在零信任架构中，应用、服务、接口、数据都可以视作业务资源。通过构建保护面实现对暴露面的收缩，要求所有业务默认隐藏，根据授权结果进行最小程度的开放，所有的业务访问请求都应该进行全流量加密和强制授权，业务安全访问相关机制需要尽可能工作在应用协议层。

（3）持续信任评估

持续信任评估是零信任体系从零开始构建信任的关键手段，通过信任评估模型和算

[4] 埃文•吉尔曼，道格•巴斯. 零信任网 络在不可信网络中构建安全系统[M].北京:人民邮电出版社,2019:40.

© 2020 奇安信集团 保留所有权利

奇安信身份安全实验室出品

法，实现基于身份的信任评估能力，同时需要对访问的上下文环境进行风险判定，对访问请求进行异常行为识别，并对信任评估结果进行调整。前文提到，在零信任架构中，访问主体是人、设备和应用程序三者结合构成的网络代理，因此在基础的身份信任的基础上，还需要评估主体信任，主体信任是对身份信任在当前访问上下文中的动态调整，和认证强度、风险状态和环境因素等相关，身份信任相对稳定，而主体信任和网络代理一样，具有短时性特征，是一种动态信任，基于主体的信任等级进行动态访问控制也是零信任的本质所在。

（4）动态访问控制

动态访问控制是零信任架构的安全闭环能力的重要体现。建议通过 RBAC 和 ABAC 的组合授权实现灵活的访问控制基线，基于信任等级实现分级的业务访问，同时，当访问上下文和环境存在风险时，需要对访问权限进行实时干预并评估是否对访问主体的信任进行降级。

3.2 零信任架构的基本原则

在零信任架构中，上述四大关键能力需要通过架构组件、交互逻辑等进行支撑。在将安全能力进行架构映射的过程中，需要遵循一些基本架构原则，才能确保最终实现的零信任架构能切实满足新型关键信息基础设施的安全保护需求，这些基本架构原则包括：

（1）全面身份化原则

对所有的访问主体需要进行身份化，包括人员、设备等，仅仅对人员进行身份管理是远远不够的；另外，访问控制的主体是网络代理，而不是孤立的人员或设备。

（2）应用级控制原则

业务访问需要尽可能工作在应用层而不是网络层，通常采用应用代理实现；应用代理需要做到全流量代理和加密，切忌不可只对应用的认证请求进行代理。

（3）安全可闭环原则

信任等级基于访问主体的属性、行为和访问上下文进行评估，并且基于信任等级对访问权限进行动态的、近实时的、自动的调整，形成自动安全闭环。

（4）业务强聚合原则

零信任架构具有内生安全属性，需要结合实际的业务场景和安全现状进行零信任架构的设计，建议将零信任安全和业务同步进行规划。零信任架构需要具备较强的适应性，能根据实际场景需求进行裁剪或扩展。

（5）多场景覆盖原则

现代关键信息基础设施具有多样的业务访问场景，如用户访问业务、服务 API 调用、

奇安信身份安全实验室出品

数据中心服务互访等场景，接入终端包括移动终端、PC 终端、物联终端等，业务部署位置也多种多样。零信任架构需要考虑对各类场景的覆盖并确保具备较强的可扩展性，以便为各业务场景实现统一的安全能力。

（6）组件高联动原则

零信任各架构组件应该具备较高的联动性，各组件相互调用形成一个整体，缓解各类威胁并形成安全闭环。在零信任架构实践中，切忌不可堆砌拼凑产品组件，各产品的可联动性是零信任能力实现效果的重要基础。

3.3 零信任架构的参考框架

零信任架构的关键能力需要通过具体的逻辑架构组件来实现，其逻辑组件参考框架如图 2 所示：

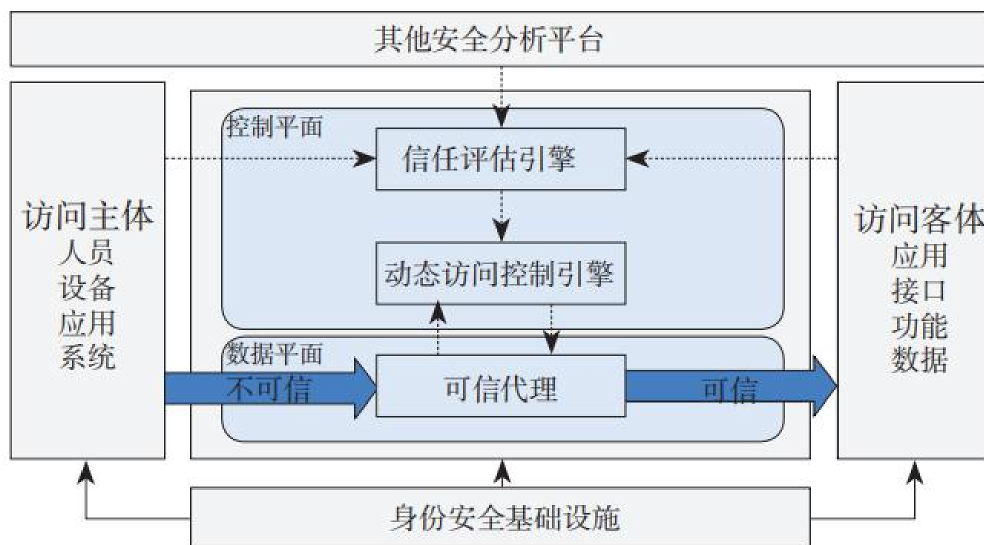


图 2 零信任通用参考框架

（1）可信代理

可信代理是零信任架构的数据平面组件，是确保业务安全访问的第一道关口，是动态访问控制能力的策略执行点。

可信代理拦截访问请求后，通过动态访问控制引擎对访问主体进行认证，对访问主体的权限进行动态判定。只有认证通过、并且具有访问权限的访问请求才予以放行。同时，可信代理需要对所有的访问流量进行加密。全流量加密对可信代理也提出了高性能和高伸缩性的需求，支持水平扩展是零信任可信代理必须具备的核心能力。

（2）动态访问控制引擎

动态访问控制引擎和可信代理联动，对所有访问请求进行认证和动态授权，是零信

© 2020 奇安信集团 保留所有权利

任架构控制平面的策略判定点。

动态访问控制引擎对所有的访问请求进行权限判定，权限判定不再基于简单的静态规则，而是基于上下文属性、信任等级和安全策略进行动态判定。动态访问控制进行权限判定的依据是身份库、权限库和信任库。其中身份库提供访问主体的身份属性，权限库提供基础的权限基线，信任库则由身份分析引擎通过实时的风险多维关联和信任评估进行持续维护。

（3）信任评估引擎

信任评估引擎是零信任架构中实现持续信任评估能力的核心组件，和动态访问控制引擎联动，为其提供信任等级评估作为授权判定依据。

信任评估引擎持续接收可信代理、动态访问控制引擎的日志信息，结合身份库、权限库数据，基于大数据和人工智能技术，对身份进行持续画像，对访问行为进行持续分析，对信任进行持续评估，最终生成和维护信任库，为动态访问控制引擎提供决策依据。另外，信任评估引擎也可以接收外部安全分析平台的分析结果，包括：终端可信环境感知、持续威胁检测、态势感知等安全分析平台，这些外部风险源可以很好地补充身份分析所需的场景数据，丰富上下文，从而进行更精准的风险识别和信任评估。

（4）身份安全基础设施

身份基础设施是实现零信任架构以身份为基石能力的关键支撑组件，至少包含身份管理和权限管理功能组件，通过身份管理实现各种实体的身份化及身份生命周期管理，通过权限管理，对授权策略进行细粒度的管理和跟踪分析。

现代关键信息基础设施已经呈现出多样化、复杂化的趋势，而传统的静态、封闭的身份与权限管理机制已经不能满足新技术环境的要求，零信任架构的身份安全基础设施需要足够灵活和敏捷，能够为更多新的场景和应用进行身份和权限管理。另外，为了提高管理效率，自助服务和工作流引擎等现代身份管理的关键能力也必不可少。

4. 零信任架构的内生安全机制

“内生安全”指的是不断从信息化系统内生长出的一种安全能力，能伴随业务的增长而持续提升，持续保证业务安全，具有自适应、自主、自生长 3 个特点。聚合是实现“内生安全”的必要手段，信息化系统和安全系统的聚合，产生自适应安全能力；业务数据和安全数据的聚合，产生自主安全能力；IT 人才和安全人才的聚合，产生自生长的安全能力。[5]

在关键信息基础设施保护能力建设过程中，要基于叠加演进原则，通过体系化的能力建设，保证信息化系统的内生安全能力有效落地。关键信息基础设施要应对多样化、未知性威胁，要将只是防御外部威胁的安全思路，扩展到基于零信任架构构建动态、可

[5] 内生安全[EB/OL].(2019-08-28)[2019-11-05].

© 2020 奇安信集团 保留所有权利

信的访问控制体系，将新的防线构建在身份、数据、业务应用上，从而不仅抵御外部威胁，更能解决由于凭证窃取及异常行为等所产生的内部威胁问题。

零信任架构聚焦身份、信任、访问控制、权限等维度的安全能力，而这些安全能力也是信息化业务系统不可或缺的组成部分，所以零信任天生就是一种“内生安全”。

作为一种“内生安全”，零信任具备自适应的能力。零信任基于业务场景的人、设备、流程、访问、环境等多维的因素，对访问主体的风险和信任度进行持续度量和评估，并通过信任等级对权限进行动态调整，这是一种动态自适应的安全闭环体系，对未知威胁的缓解具有很强的自适应性。零信任的落地实现需要结合企业信息化业务系统的现状和需求，把零信任的核心能力和产品技术组件内嵌入业务系统，构建自适应“内生安全”机制。因此，建议在业务系统规划建设之初同步进行零信任架构的规划设计，实现安全系统和业务系统的深入聚合。

同时，零信任架构方案的部署实施要求企业的业务团队、IT 团队以及安全团队的人员紧密配合、协同合作，形成合力，而不能像过去一样分开自治，这些人才的聚合是零信任架构解决方案成功落地的有效保障。零信任提供的自适应的访问控制能力是开放的、平台化的，企业可以将业务逐步迁移到零信任，迁入的业务都将具备这种自适应的安全能力，这样零信任就变成了企业业务流程的内生能力，持续为企业的网络安全赋能。

5. 结束语

零信任安全架构对传统的边界安全架构思想重新进行了评估和审视，并对安全架构思路给出了新的建议：默认情况下不应该信任网络内部和外部的任何人、设备、系统和应用，而是应该基于认证、授权和加密技术重构访问控制的信任基础，并且这种授权和信任不是静态的，它需要基于对访问主体的风险度量进行动态调整。安全与关键信息基础设施建设应如同 DNA 的双链，相辅相成，而它们的关键结合点，就是在同步规划、同步建设、同步运行 3 个关键点上，从而做到两者的深度融合，全面覆盖，实战化运行，协同响应。要从应对局部威胁和合规点的建设模式，走向面向能力导向建设模式，关口前移，构建“内生安全”能力，为关键信息基础设施的核心数据与业务运营提供保障。零信任架构认为不应该仅仅在企业网络边界上进行粗粒度的访问控制，而是应该对企业的人员、设备、业务应用、数据资产之间的所有访问请求进行细粒度的访问控制，并且访问控制策略需要基于对请求上下文的信任评估进行动态调整，是一种应对新型 IT 环境下已知和未知威胁的“内生安全”机制，具有更好的弹性和自适应性。

参考文献：

1 奇安信韩永刚：内生安全助力关键信息基础设施保护 - 中国青年网
[EB/OL].(2019-10-30)[2019-11-05].
http://d.youth.cn/shrgch/201910/t20191030_12106997.htm

© 2020 奇安信集团 保留所有权利

2 埃文•吉尔曼，道格•巴斯. 零信任网络 在不可信网络中构建安全系统[M].北京:人民邮电出版社,2019:1~2.
3 网络安全架构：零信任架构正在标准化:安全内参 [EB/OL].(2019-09-28)[2019-11-05]. https://www.secrss.com/articles/14045.
4 埃文•吉尔曼，道格•巴斯. 零信任网 络在不可信网络中构建安全系统[M].北京:人民邮电出版社,2019:40.
5 内生安全[EB/OL].(2019-08-28)[2019-11-05]. https://baike.baidu.com/item/%E5%86%85%E7%94%9F%E5%AE%89%E5%85%A8.

（文章首发:《保密科学技术》杂志 2019 年 11 月刊，内容有部分修订）

奇安信身份安全实验室出品

零信任迁移方法论

零信任架构作为一种全新的安全架构，和企业现有的业务情况、安全能力、组织架构都有一定的关系，零信任迁移不可能一蹴而就，需要遵循一定的方法论，结合企业现状，统一目标和愿景后进行妥善规划并分步建设。

零信任迁移方法如图所示：

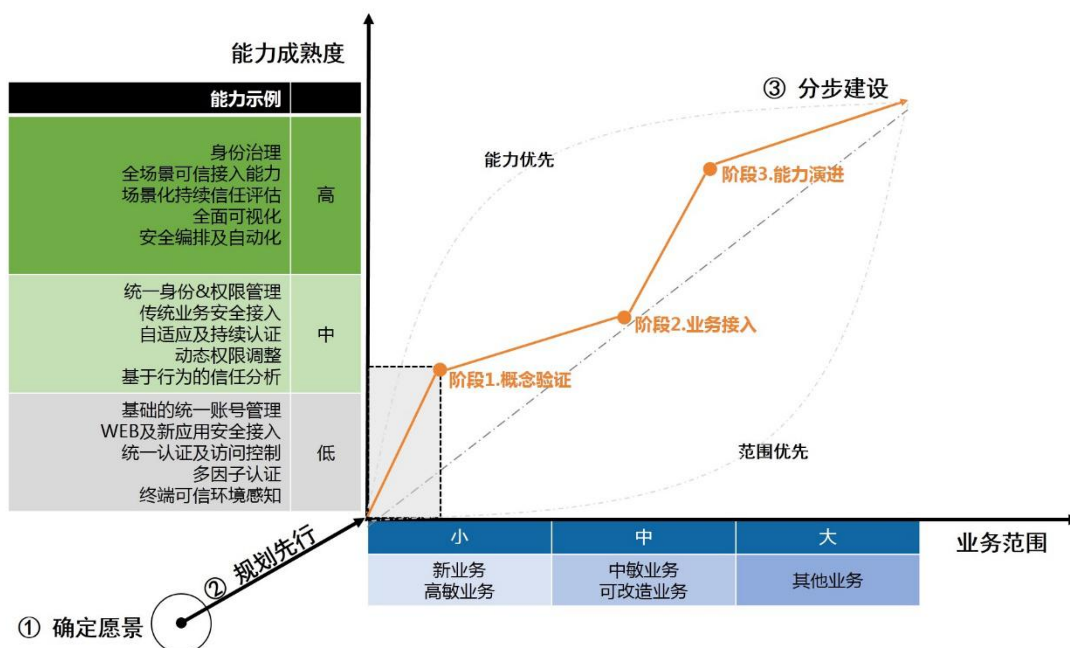


图 零信任迁移方法

▪ 确定愿景

零信任的建设和运营需要企业各干系方积极参与，可能涉及到安全部门、业务开发部门、IT 技术服务部门和 IT 运营部门等。企业数字化转型的关键决策者应该将基于零信任的新一代安全架构上升到战略层面，确定统一的愿景，建议成立专门的组织（或虚拟组织）并指派具有足够权限的人作为负责人进行零信任迁移工作的整体推进，建议至少由 CIO/CSO 或 CISO 级别的人员在公司高层决策者的支持下推动零信任项目。

需要特别注意的是，在很多企业安全部门话语权并不高，安全项目往往受到业务部门的阻碍甚至反对，零信任项目的发起者一定需要从零信任的业务价值出发，说服业务部门和公司的高层决策者。

另外，在零信任的迁移过程中，需要更多部门和人员的配合和支持，特别是大量的普通员工，他们作为零信任项目的最终使用者，他们的支持至关重要，建议通过公司级的持续的安全文化活动加强全体人员对零信任安全的认可，这一点也至关重要。

© 2020 奇安信集团 保留所有权利

▪ 规划先行

零信任架构是安全思维和安全架构进化的必然，聚焦身份、业务、信任和动态访问控制等维度的安全能力，而这些能力业务密不可分，所以零信任天生就应该是一种内生安全。零信任的建设路径需要结合现状和需求，将零信任的核心能力和组件内嵌入业务体系，构建自适应内生安全机制，建议在业务建设之初进行同步规划，进行安全和业务的深入聚合。

规划的目的在于厘清形状，确定路径。对于零信任架构而言，需要从两个维度进行梳理和评估，一是能力成熟度维度，一是业务范围维度。

零信任架构的关键能力包括：以身份为基石、业务安全访问、持续信任评估和动态访问控制，每一项关键能力又可以划分为若干子能力，企业需要评估当前具备的安全能力，并基于风险、安全预算、合规要求等信息，确定安全能力建设的优先级。

零信任架构最终需要覆盖企业的所有资源，为其构建保护面。企业资源包括但不限于：应用、接口、功能和数据等。在规划阶段，需要确定迁移至零信任的业务优先级。一般来说新建业务和核心业务作为第一优先级考虑。

对安全能力现状、需求，业务现状、优先级进行梳理后，需要进一步对核心业务的暴露面进行梳理，对各暴露面的访问主体、访问主体的权限进行梳理，确定初步的总体建设路径及第一阶段建设方案。

▪ 分步建设

规划完成后进入建设阶段，根据规划的思路导向，建设阶段的划分依各企业而各有不同。如果是能力优先型建设思路，需要针对少量的业务构建从低到高的能力，通过局部业务场景验证零信任的完整能力，然后逐步迁移更多的业务。范围优先型则先在一个适中的能力维度上，迁移尽量多的业务，然后再逐步对能力进行提升。两种建设思路各有侧重，依据企业的具体情况，在规划阶段选定思路和建设阶段的划分。

一种建议的分步思路主要包含三个阶段：概念验证、业务接入和能力演进。首先在一个较小业务范围内，构建中等的零信任安全能力，对整体方案进行验证；方案验证完成后，对验证过程的一些局部优化点进行能力优化，并同时迁入更多的业务进一步验证方案并发现新的安全需求；最后，基于验证结果规划后续能力演进阶段，逐步有序的提升各方面的零信任能力。

零信任架构作为一种全新的安全思路，是持续演进的过程，需要基于业务需求、安全运营现状、技术发展趋势等对零信任能力进行持续完善和演进。

（文章节选自：Gartner&奇安信《零信任架构及解决方案》联合白皮书）

奇安信身份安全实验室出品

BeyondProd：一种新的云原生安全方法

▪ 编者按

新一代网络安全方法已经超越了传统的基于边界的安全模型，在传统的基于边界的安全模型中，“墙”可以保护边界，并且内部的任何用户或服务都将受到完全信任。在云原生环境中，仍然需要保护网络外围，但是仅靠这种安全方法还远远不够——如果防火墙不能完全保护公司网络，那么它也不能完全保护生产网络。

云原生技术有利于各组织在公有云、私有云和混合云等新型动态环境中，构建和运行可弹性扩展的应用。云原生的代表技术包括容器、服务网格、微服务、不可变基础设施和声明式 API。这些技术能够构建容错性好、易于管理和便于观察的松耦合系统。结合可靠的自动化手段，云原生技术使工程师能够轻松地对系统作出频繁和可预测的重大变更。

2014 年，Google 开始对外介绍 BeyondCorp，这是一种用于用户访问企业网络的网络安全模型。BeyondCorp 基于零信任架构原则，重新定义了企业网络访问。在此同时，谷歌同样还将零信任架构应用于其如何连接机器，工作负载与服务之中。这个项目就是 BeyondProd。

在 BeyondProd 中，谷歌设计并实践了以下安全原则：

- 在边缘保护网络；
- 服务间默认不互信；
- 在可信机器上运行来源已知的代码；
- 跨服务强制执行一致策略的关卡；
- 发布流程更改实现简单化、自动化及标准化；
- 工作负载之间进行隔离。

简言之，谷歌通过多种控件和模块，实现容器及在其中运行的微服务能够安全部署，彼此间安全通信，彼此相邻安全运行，而不会给单个微服务开发人员增加基础架构的安全性和实现细节的负担。

▪ BeyondProd：一种新的云原生安全方法

谷歌在此前已经撰写了几篇白皮书来介绍有助于提高安全性的谷歌内部开发项目。在本文中，BeyondProd 特意沿用了 BeyondCorp 的概念——正如边界安全模型不再适用于终端用户一样，它也同样不再适用于微服务场景。对照 BeyondCorp 文中的话来讲：“此

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

模型的关键假设不再成立：边界不再仅仅是企业[数据中心]的实际位置，且边界内的区域也不再是托管个人计算设备和企业应用程序[微服务]的安全可靠之处。”

本文将详细介绍，谷歌的多个基础架构是如何在一个如今被称为“云原生（cloud-native）”的架构中进行协同工作来保护工作负载（workload）的。有关谷歌安全的概述，可参阅《安全架构设计白皮书》。

本文记录内容截至到 2019 年 12 月是正确无误的。本文仅代表截止撰文时的状态。随着谷歌持续改善对用户的保护机制，谷歌云的安全政策和系统未来可能会发生变化。

▪ 术语库

本文采用以下定义：

- **微服务（microservice）**将应用需要执行的单个任务（task）分离成多个单独的服务（service），每个服务都可独立进行开发和管理，并具有自己的 API、发布环节、扩展和配额管理。在更现代化的体系架构中，一个应用（如一个网站）可以作为微服务的集合而运行，而不再作为某个单体应用。微服务具有独立化、模块化、动态化和短时化的特征。它们可分布在众多主机、集群，乃至云端。
- **工作负载（workload）**是应用完成的特有任务。在微服务架构中，工作负载可以是一个或多个微服务。
- **作业（job）**是运行一个应用某个部分的单个微服务实例。
- 微服务使用**服务身份（service identity）**向基础架构中运行的其他服务证明自己身份。
- **服务网格（service mesh）**是服务和服务间通信的基础架构层，可以控制流量、应用策略和集中监控服务调用。使用微服务架构时，可以消除由单个服务执行这些控制措施的负担，并允许跨多个微服务进行更简单的集中管理。

▪ 面向 CIO 的概要

- 谷歌的基础架构将工作负载作为单独的微服务部署在容器中，并使用 Borg（谷歌的容器编排系统）来管理这些工作负载。这就是如今众所周知的“云原生”架构的灵感和模版来源。
- 谷歌的基础架构在设计之初就将安全性纳入考虑，而不是在事后补充。谷歌的基础架构默认假定各服务之间互不信任。
- 谷歌通过一项名为 BeyondProd 的计划来保护微服务。保护内容包括如何更改代码以及如何访问微服务中的用户数据。BeyondProd 应用的概念包括：进行双向身份认证的服务端点、传输安全、具备全局负载均衡和拒绝服务防护能力的边缘终结、端到端源代码溯源和运行时沙箱。
- 从传统的安全模型向云原生安全模型迁移，需要对基础架构和开发过程这两个主要方面进行更改。在包含和连接所有微服务的共享结构（也称为服务网格）中构建共享组件，可以更轻松地发布变更并实现跨服务的一致安全性。

奇安信安全研究院出品

▪ 动机

谷歌向容器化和容器编排化演进，是为了获得更高的资源利用率，构建高可用的应用，并简化谷歌开发人员的工作。促使谷歌向容器化基础架构演进的另一个理由是为了让我们的安全控制措施与架构保持一致。我们已经清楚地认识到，以网络边界为中心的安全模型不够安全。一旦攻击者突破了边界，就可以在网络中畅行无阻。虽然我们意识到需要加强整个基础架构中的安全控制措施，但同时也希望谷歌的开发人员能够轻松编写和部署安全的应用，而不必自己动手去实现这些安全能力。

从单体应用演进到使用编排系统从容器部署的分布式微服务有着明显的操作优势：让管理和扩展更为简单。这种云原生架构需要使用不同的安全模型和不同的工具来实现保护与微服务的管理和可扩展优势协调一致的部署。

本文将描述谷歌如何实施云原生安全，即 BeyondProd：转变到云原生架构对安全的意义，云原生安全的安全原则，为满足这些需求而构建的系统，以及各位读者将如何在自身实现类似改变的一些指南。

▪ 谷歌的云原生安全

容器化微服务

自公司成立初期，谷歌就有意识地决定采用低成本的商用服务器来扩大数据中心的容量，而不是投资价格昂贵的高可用性硬件。我们一直以来、并将在未来持续实践一套可靠的指导原则，即系统任何单一部分发生故障都不应影响用户所能看到的服务的可用性。要实现这种可用性，需要运行冗余的服务实例，这样单个故障的发生才不会导致服务中断。基于这种原则，我们才开发了容器、微服务及容器编排技术，以灵活管理这些高度冗余和分布式系统的部署。

容器化的基础架构意味着每个工作负载都要部署一组属于自己的不可变、可移动、可调度的容器。为了在内部管理这些容器，我们开发了一套名为 Borg 的容器编排系统[1]，目前我们仍通过它来实现每周部署数十亿个容器。

容器使得工作负载更易于在机器之间进行封装和重新调度。微服务使开发和调试应用的不同部分变得更容易。将微服务和容器两者结合使用，可以将工作负载拆分成更小、更易于管理的单元，以便进行维护和发现。采用具有微服务架构的容器化基础架构被称为采用“云原生”。服务在 Borg 部署的容器中运行。该架构可以根据需要扩展工作负载——如果对特定工作负载有很高的需求，则可能有多台计算机运行同一服务的副本以处理所需规模的工作负载。

谷歌的一个与众不同之处就在于，我们在架构的每一次演进中都考虑到了安全性。最新的这个云原生安全的概念与谷歌多年来用于保护基础架构的理念相当。我们微服务体系架构和开发过程的目标是在开发和部署生命周期中尽早解决安全问题——在这个阶段解决问题的成本较低——并通过保持标准和持续一致的方式加以解决。最终的结果是，开发人员在确保安全性方面花费的时间更少，同时仍然能获得更安全的效果。

奇安信安全实验室出品

迁移到云原生架构

现代的安全体系架构已经超越了基于边界的传统安全模型——采用防火墙保护边界，完全信任防火墙内部的任何用户或服务。BeyondCorp 项目即现代企业用户的工作方式变化的一种应对方式。如今，用户采用移动办公方式，常常会在组织的传统安全边界之外工作，例如在咖啡店、飞机或其他的任何地方。在 BeyondCorp 中，我们放弃了特权企业网络的概念，并且仅基于设备和用户凭据和属性进行授权访问，不管用户的网络位置如何。

云原生安全解决了服务及其用户所面临的共同问题——在云原生环境中，不能仅仅依靠防火墙来保护生产网络，就像不能仅仅依赖防火墙来保护企业网络一样。正如用户并非都在使用同一个物理位置或设备一样，开发人员也并非都会将代码部署到同一个环境中。借助 BeyondProd，微服务不仅可以运行在防火墙保护下的数据中心中，还可以运行在公有云、私有云或第三方托管服务中，并且在任何地方都能确保它们的安全。

正如用户会移动、会使用不同的设备、会从不同的位置连接一样；微服务也会移动、会跨异构主机、会部署在不同的环境中。BeyondCorp 认为"*用户信任应取决于**设备的上下文感知状态**等特性，而不应取决于连接到公司网络的权限*"，与此对应，BeyondProd 认为"***服务信任**应取决于**代码来源和服务身份**等特性，而不应取决于在生产网络中的位置，如 IP 或主机名身份*"。

云原生架构和应用开发

只专注于基于边界的安全作为一种相对更传统的安全模型，无法独立保护云原生架构。举个例子，采用三层架构的单体应用被部署到公司的私有数据中心，该中心有足够的容量来处理关键事件的峰值负载。对硬件和网络有特定要求的应用会特意部署到通常保留固定 IP 地址的特定机器上。更新的发布频率较低、规模较大，且很难协调，因为更新所带来的更改会同时影响应用的许多部分。这会导致应用的生命周期过长，而且更新频率较低，同时使用安全补丁的频率也通常较低。

但是，在云原生模型中，容器将应用所需的二进制文件与底层主机操作系统分离，使应用更具可移植性。容器的不可变性意味着它们一旦部署就不会发生更改——因此它们可以被频繁地重新构建及重新部署。作业具有可扩展性可以很好地处理负载：在负载增加时可部署新的作业，当负载减少时可终止现有作业。由于容器会频繁重启、终止或重新调度，因此硬件和网络的重复使用和共享会更加频繁。采用通用的标准化构建和分发流程，会使得团队之间的开发流程更一致、统一，即使团队独立管理其微服务的开发也是如此。因此，安全考虑（例如安全审核、代码扫描和漏洞管理）可以在开发周期的早期阶段进行。

对安全的影响

前面已经详细介绍了关于内部不可信的模型——类似 BeyondCorp 中的用户——可以如何应用到 BeyondProd 中的微服务，但这种转变究竟是怎样的？下表 1 对传统基础架构的安全性方面与云原生架构中的安全性方面的不同进行了对比。表 1 还描述了从传

© 2020 奇安信集团 保留所有权利

统架构迁移到云原生架构需要满足的相关要求。本节其余部分为针对表的每一项进行详细描述。

传统基础架构安全性	云原生安全性	云原生安全性的隐含要求
基于边界的安全（如防火墙），其内部通信默认安全。	零信任安全，对服务之间的通信进行验证，环境中的服务没有隐式信任。	对网络边界的防护依然有效，但服务间没有默认互相信任。
某些应用使用固定 IP 和专用硬件。	包括 IP 和硬件在内的更高资源利用率、复用率、和共享率。	运行已知出处的代码可信机器。
基于 IP 地址的身份。	基于服务的身份。	
服务在已知预期的位置运行。	服务可以在环境中的任何位置运行，包括跨公有云和私有数据中心混合部署。	
每个应用都内置了特定安全要求，且这些要求会单独分别执行。	遵循集中式强制策略，服务栈中集成了共享的安全性要求。	用于跨服务强制执行持续一致策略的关卡。
对如何构建和审核服务的限制有限。	对所有的服务采用持续一致的安全要求。	
对安全组件的监督有限。	集中的安全策略视图及遵守策略的情况。	
专门发布更新，发布频率较低。	标准化构建和发布过程，更改单个微服务更频繁。	发布流程更改实现简单化、自动化及标准化。
工作负载通常作为 VM 部署或部署到物理主机，并使用物理机或 hypervisor 来提供隔离。	封装的工作负载及其进程在共享的操作系统中运行，则需要一种隔离工作负载的机制。	对共享操作系统的工作负载进行隔离。

表 1：迁移到云原生架构时隐含的安全性要求

从基于边界的安全到零信任安全

在传统的安全模型中，组织的应用可以依赖其私有化数据中心周围的外部防火墙来防护入站流量。但在云原生环境中，尽管像在 BeyondCorp 模型中一样仍然需要保护网络边界，但仅基于边界的安全模型已经远不再安全。这并不是在说我们遇到了新的安全问题，而是会让人注意到一个事实：如果防火墙无法完全保护企业网络，它就无法完全保护生产网络。在零信任安全模型中，无法再对内部流量保留隐式信任——它需要其他安全控制措施，如身份认证和加密。同时，向微服务的转变提供了重新思考传统安全模型的机会。当消除对单一网络边界（如防火墙）的依赖时，就可以按服务进一步划分网络。进一步来说，可以进行微服务级别的分段，使得服务间没有固有的信任。通过微服务，流量可以有不同的信任级别并且使用不同的控制措施——不再只是比较内部流量与外部流量。

© 2020 奇安信集团 保留所有权利

从固定 IP 地址和硬件到更大的共享资源

在传统安全模型中，组织的应用部署在专用机器上，且这些机器的 IP 地址不常变化。这意味着安全工具可以靠相对静态的架构映射，通过可预测的方式关联应用——如防火墙等工具中的安全策略可以用 IP 地址作为标识符。

但是，在云原生环境中，由于共享主机和频繁更改的作业，通过防火墙来控制服务间访问的方式行不通。特定 IP 地址与特定服务相关联的设定将不再有效。因此，身份应基于服务，而不应基于 IP 地址或主机名。

从特定于应用的安全实施到集成在服务堆栈中的共享安全要求

在传统安全模型中，每个应用只负责满足自身的安全要求，而不用考虑其他的服务。这些要求包括身份管理、SSL/TLS 终止和数据访问管理。这常常导致实施方式不一致或安全问题得不到解决，并且由于在很多地方都需要解决这些问题，这就使得修复措施更难实现。

在云原生环境中，服务之间会更频繁地重复使用组件，并且会有关卡来确保跨服务一致强制执行政策。可以通过不同的安全服务来执行不同的安全策略。与其要求每个应用分别实现关键的安全服务，不如将不同的安全策略拆分为单独的微服务（例如，一个策略用于确保对用户数据的授权访问，另一个策略用于确保使用最新的 TLS 密码套件）。

发布流程从定制更新且频率较低到标准更新且频率更高

在传统安全模型中，共享服务很有限。如果代码分散各处，加上本地化开发，意味着很难确定涉及应用许多部分的更改所造成的影响——因此，更新的发布频率较低且难以协调。要进行更改，开发人员可能需要直接更新每个组件（例如，通过 SSH 连接到虚拟机来更新配置）。总的来说，这会导致某些应用的生命周期变得过长。从安全性角度来看，由于代码更分散，因此审核难度更大，而且更难确保在修复漏洞时，在任何地方都能修复该漏洞。迁移到频繁、标准化发布更新的云原生架构后，安全设计在软件开发生命周期中的位置会左移[2]。这样可以实现更简单、更一致的安全性强制执行措施，包括定期应用安全补丁程序。

从使用物理机或 hypervisor 进行工作负载隔离到需要更强的隔离能力使得可在同一台机器上运行封装式工作负载

在传统安全模型中，工作负载被调度到自己的实例上，没有共享资源。应用被机器和网络边界有效隔开，工作负载隔离完全依靠物理主机不同、hypervisor（虚拟机监控程序）和传统防火墙来实现。

在云原生环境中，工作负载装入容器并封装到共享主机和共享资源上。因此，需要在工作负载之间建立更强的隔离。在使用网络控制和沙箱技术的部分中，工作负载可以

奇安信安全专家出品

© 2020 奇安信集团 保留所有权利

分离为彼此隔离的微服务。

安全原则

在开发云原生架构的同时希望增强其安全性——因此我们制定并优化了以下安全原则：

- **在边缘保护网络**，使工作负载与来自互联网的网络攻击和未经授权流量隔离开。虽然基于防火墙的方法不是云原生架构的新概念，但它仍不失为一种有效安全实践。在云原生环境中，通过基于边界的防护方法用来保护尽可能多的基础架构，使其避开来自互联网的未经授权的流量和来潜在的攻击，例如基于容量的拒绝服务攻击。
- **服务间默认不互信**，只有已知的、可信的和明确授权的调用者才能使用服务。这可以阻止攻击者使用不可信代码访问服务。如果某项服务确实被破坏，这会阻止攻击者执行允许其扩大访问范围的操作。这种互不信任有助于限制破坏的爆炸半径。
- **在可信机器上运行来源已知的代码**，因此服务身份仅限于使用授权代码和配置，并且只能在经过验证的、授权环境中运行。
- **跨服务强制执行一致策略的关卡**。例如，一个用于验证访问用户数据请求的关卡，如此服务的访问来自获得授权的最终用户发出且经过验证的请求，并且管理员的访问需要提供正当的理由。
- **发布流程更改实现简单化、自动化及标准化**，以便相关人员轻松审核基础架构更改对安全性的影响，并且可以在几乎不影响生产环境的情况下发布安全补丁程序。
- **共享操作系统的工作负载之间的隔离**，如果一个服务被破坏，不会影响在同一台主机上运行的其他工作负载的安全性。这限制了潜在破坏的“爆炸半径”。

在整个基础架构中，我们的目标是实现不依赖于人的自动化安全。安全的扩展方式应与服务的扩展方式相同。在默认情况下，服务应该是安全的；在异常情况下，服务应该是不安全的——人工操作应该异常情况下进行，而不是作为日常事务，并且人工操作应该可审核。然后，我们可以根据为某项服务部署的代码和配置而不是部署服务的人员来对服务进行身份认证。

综上，这些安全原则的实施意味着容器和运行在其中的微服务可以部署、相互通信及并行运行，而不削弱云原生架构的属性（即简单的工作负载管理、可无运维扩展和有效封装）。所有这些都可以实现，而无需再向单个微服务开发人员提供底层基础架构的安全属性和实现细节。

谷歌的内部安全服务

为了保护谷歌的云原生架构，我们设计并开发了多种内部工具和服务。下列安全服务都用于实现上节“安全原则”中定义的相关安全原则：

- 谷歌前端（Google Front End，GFE）：终止来自最终用户的连接，并为强制执行 TLS 最佳实践提供了一个中心点。尽管我们不再强调基于边界的安全模型，但 GFE 仍然是保护内部服务免受拒绝服务攻击的重要策略部分。GFE 是用户连接谷歌网络的第一个入口点；在基础架构中，GFE 还根据需要在区域之间平衡负载和重新路由流量。GFE 是将流量路由到适当微服务的边缘代理。
- 应用层传输安全（Application Layer Transport Security，ALTS）：用于 RPC 身

© 2020 奇安信集团 保留所有权利

份验证、完整性和加密。ALTS 是谷歌基础架构中服务间相互认证和传输加密的系统。身份通常绑定到服务，而不是绑定到特定的服务器名或主机。这有助于实现跨主机的无缝微服务复制、负载平衡和重新调度。

- **Borg 的二进制授权（Binary Authorization for Borg）**和**主机完整性（Host Integrity）**分别用于微服务和机器完整性验证：
  - Borg 的二进制授权（BAB）：在部署时进行强制检查可以确保代码在部署前满足内部安全要求。BAB 检查包括由另一名工程师审核更改的内容、将代码提交到源代码库以及在专用基础架构上以可验证的方式构建二进制文件。在谷歌的基础架构中，BAB 限制未经授权的微服务的部署。
  - **主机完整性（HINT）**：通过安全引导过程验证主机系统软件的完整性，并基于受支持的安全微控制器硬件运行。主机完整性检查包括在 BIOS、BMC、bootloader（引导加载程序）和 OS 内核上验证数字签名。
- **服务访问策略（Service Access Policy）**和**最终用户上下文票据（End user context tickets）**用于限制对数据的访问：
  - 服务访问策略：限制服务间数据的访问方式。当 RPC 从一个服务发送到另一个服务时，服务访问策略会定义访问接收服务的数据所需的身份验证、授权和审核策略。这将限制数据的访问方式，授予所需的最低访问权限级别，以及指定如何审核访问权限。在谷歌的基础架构中，服务访问策略会限制一个微服务访问另一个微服务的数据，并允许对访问控制进行全局分析。
  - 最终用户上下文（EUC）票据：这些票据由最终用户身份认证服务颁发，为服务提供用户身份（不同于服务身份）。这些票据受到完整性保护、集中颁发、支持转发，用于证明请求服务的最终用户身份。这样可以减少服务间的信任需求，因为通过 ALTS 验证的对等方身份通常不足以授予访问权限，此类授权决策通常也基于最终用户的身份。
- **用于蓝/绿部署的 Borg 工具**[3]：此工具负责在执行维护任务时迁移正在运行的工作负载。除现有的 Borg 作业之外，还部署了新的 Borg 作业，并且负载平衡会逐渐将流量从一个作业迁移到另一个作业。这样就可以在不停机且用户无感知的情况下对微服务进行更新。此工具可以用于在我们添加新功能时应用服务升级，以及在保证不停机的情况下完成关键的安全更新（例如，针对 Heartbleed 和 Spectre/Meltown 漏洞的安全更新。对于影响谷歌云基础架构的更改，我们使用实时迁移来确保 VM 工作负载不受影响。
- gVisor，用于工作负载隔离。gVisor 使用用户空间内核来拦截和处理系统调用，从而减少了与主机间和潜在的攻击面的交互。此内核提供了运行应用所需的大部分功能，并限制应用可访问的主机内核面。在谷歌的基础架构中，gVisor 是用于隔离在同一主机上运行的内部工作负载和谷歌云客户工作负载的几个重要工具之一。

下表 2 列出了在“安全原则”一节中描述的每个原则与谷歌用于实现该原则的相应工具的对应关系。

安全原则	**谷歌的内部安全工具/服务**
在边缘保护网络	**谷歌前端（GFE）**，用于管理 TLS 终止和入站流量的策略
服务间默认不互信	**应用层传输安全性（ALTS）**，用于 RPC 身

	份认证、完整性、加密和服务身份
在可信机器上运行来源已知的代码	**Borg 的二进制授权（BAB）**，代码来源验证 **主机完整性（HINT）**，机器完整性验证
跨服务强制执行一致策略的关卡	**服务访问策略**，用于限制服务间的数据访问方式 **最终用户上下文（EUC）票据**，用于证明原始请求者的身份
简单、自动及标准的更改发布	**Borg 工具**，用于蓝/绿部署
共享操作系统的工作负载间的隔离	**gVisor**，用于工作负载隔离

表 2：谷歌实现云原生安全的原则及安全工具

综合应用

本节将描述前面介绍到的组件是如何组合在一起为云原生环境中的用户请求提供服务的。我们将使用两个例子：第一个，我们追踪从创建到目的地交付的典型用户数据访问请求过程；第二个，我们追踪从开发到投入生产的代码更改过程。请注意，这里将列出的技术不会都用于谷歌基础架构的所有部分——主要取决于服务和工作负载。

用户数据访问

如图 1 所示，当 GFE 接收到用户的请求时（步骤 1），它会终止 TLS 连接，并通过 ALTS[4] 将请求转发到相应的服务前端（步骤 2）。应用前端使用中央最终用户身份验证服务（EUA）认证用户的请求，如果认证成功则会接收到一个短期加密的最终用户上下文票据（EUC）（步骤 3）。

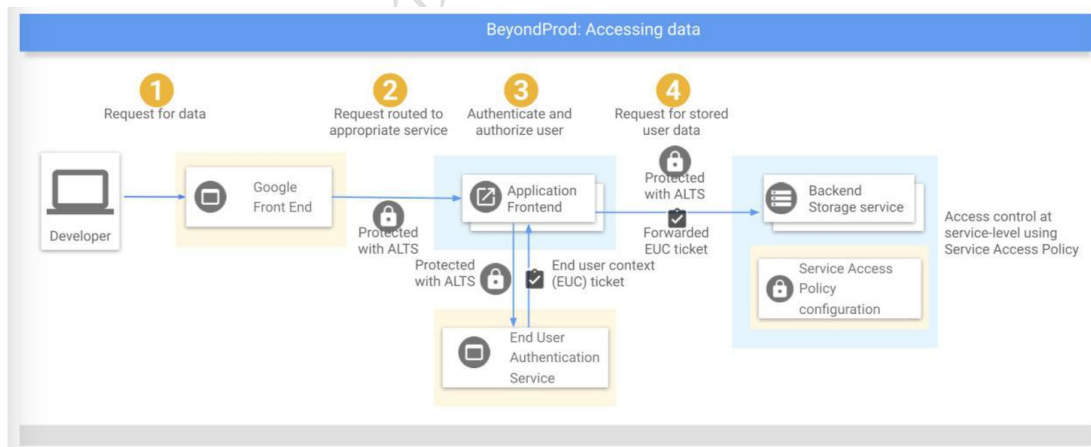


图 1：谷歌云原生架构安全控制措施——用户数据访问

然后，应用前端通过 ALTS 向存储后端服务发起 RPC 请求，从而在后端请求中转发 EUC 票证（步骤 4）。后端服务使用服务访问策略来确保：

1. 系统授权前端服务的 ALTS 身份向后端服务发出请求并提供 EUC 票据，
2. 前端的身份由 BAB 保护，
3. EUC 票据有效。

接下来，后端服务检查 EUC 票据中的用户是否有权访问请求的数据。如果检查中任

何一项失败，请求将被拒绝。在很多情况下，存在一系列后端调用，每个中间服务都对入站 RPC 执行服务访问策略检查，并在出站 RPC 上转发 EUC 票据。如果这些检查通过，则数据将返回到授权的应用前端，并提供给授权用户。

每台机器都有一个通过 HINT 系统预配的 ALTS 凭据，并且只有在 HINT 验证计算机引导成功时才能解密。大多数谷歌服务都是运行在 Borg 上的微服务，这些微服务都有自己的 ALTS 身份。Borgmaster[5]根据微服务的身份将这些 ALTS 微服务凭据授予工作负载，如图 1 所示。机器级的 ALTS 凭据构建了安全通道来预配置微服务凭据，因此只有成功通过 HINT 验证引导的机器才能实际托管微服务工作负载。

代码更改

如图 2 所示，当一个谷歌员工要更改受适当强度 BAB 保护的微服务时，必须将更改的内容提交到中央代码库执行代码审核。一旦批准，更改的内容将提交到受信任中央构建系统，该系统会生成带有签名的可验证生成清单证书的包（步骤 1）。在部署时，BAB 通过验证来自构建管道的签名证书来验证此过程（步骤 2）。

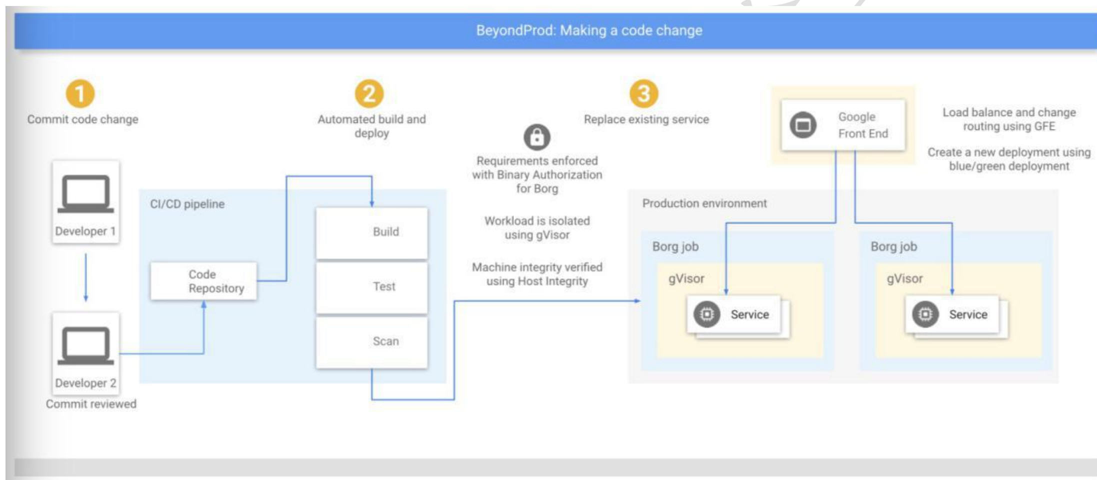


图 2: 谷歌云原生架构的安全控制措施——代码更改

无论是常规发布还是紧急安全补丁发布，所有的工作负载更新都是通过蓝/绿部署来处理的（步骤 3）。GFE 会将流量负载平衡到新部署以确保操作的连续性。

所有工作负载都需要进行隔离。如果工作负载不太可信，例如，工作负载是多租户的，或者源代码来自谷歌外部，可以将其部署到由 gVisor 保护的环境中，或者使用其他隔离层。隔离可确保在应用的一个实例受到损害时，其他实例都不会受到影响。

应用 BeyondProd

全面实施

通过采用云原生架构并有效保护基础架构，谷歌可以为内部和外部（谷歌云）的工作负载都提供非常强大的安全属性。

通过构建共享组件，满足公共安全需求对单个开发人员的负担最小。理想情况下，

© 2020 奇安信集团 保留所有权利

安全功能不需要集成到每个单独的应用中，而是作为封装和连接所有微服务的结构来提供。这种技术即通常所说的服务网格。这也意味着安全可以与常规开发或部署活动分开管理和实现。

向云原生进行转变

谷歌向云原生的转变要主要在两个方面：在基础架构中和在开发过程中。谷歌在同一时间完成了这两方面更改，但其实它们可以分开并单独完成。

更改基础架构

我们首先构建了服务身份、身份认证和授权的强大基础。有了可信服务身份作基础，就能够实现更高级别的安全功能（如服务访问策略和 EUC 票据），这些功能依赖于对服务身份的验证。为了使这种转换对于新的和现有的服务都简单，ALTS 最初作为仅包含一个助手守护进程的库提供。这个守护进程运行在每个服务都可以调用的主机上，并随着时间的推移演变为使用服务凭据的库。ALTS 库被无缝地集成到核心 RPC 库中——这使它更容易被广泛采用，而不会给各个开发团队带来很大的负担。发布 ALTS 是发布服务访问策略和 EUC 票据的前提条件。

更改开发过程

对谷歌来说，建立一个强大的构建和代码审核流程至关重要。这能够确保正在运行的服务的完整性，并确保 ALTS 使用的身份是有意义的。我们建立了一个集中式的构建流程，在其中能够开始执行要求，如在构建和部署时要求有两人参与代码审核和自动化测试。(如需了解部署的详细信息，参见 Borg 的二进制授权白皮书。

完成这些基础工作后，就着手开始解决在我们的环境中运行外部的、不可信的代码的需求。为了实现这一目标，我们开始进行沙箱测试——最初使用 ptrace，后来使用 gVisor。同样的，蓝/绿部署在安全性（例如打补丁）和可靠性方面都提供了显著的优势。

我们很快发现，如果服务一开始选择记录违反策略的行为，而不是直接阻止违反策略的行为，我们的目标会更容易实现。这种方法具有双重优势。首先，它让服务所有者有机会测试更改内容并评估迁移到云原生环境对其服务的影响（若有）。其次，它使我们能够在修复 bug 的同时找出可能需要向服务团队提供的其他功能。例如，服务登陆到 BAB 时，服务所有者会启用“仅限审核”模式。这有助于他们识别不符合要求的代码或工作流程。解决了“仅限审核”模式所标记的问题后，服务所有者会启用强制执行模式。在 gVisor 中，我们首先将工作负载装入沙箱，即使沙箱存在兼容性问题，然后系统地解决这些兼容性问题以改进沙箱，从而达到我们的目的。

© 2020 奇安信集团 保留所有权利

转变带来的好处

正如 BeyondCorp 帮助谷歌超越了基于边界的安全模型一样，BeyondProd 在生产环境安全性方面实现了类似飞跃。BeyondProd 方法描述了一种云原生安全体系架构，该架构假定服务间不存在信任，隔离工作负载，验证是否仅部署了集中构建的应用，自动执行漏洞管理以及对关键数据实施强访问控制。基于 BeyondProd 架构，谷歌开发了多个新系统来实现满足这些需求。

太多时候，对安全的考虑总是在最后时刻才被大家想起——这时往往都已经做出了迁移到一个新结构的决定。尽早让安全团队参与进来并且专注于新安全模型的优势，如更简单的补丁管理和更严格的访问控制，云原生架构可以为应用开发和安全团队带来明显的优势。将本文介绍的安全原则应用于诸位读者的云原生基础架构时，可以加强工作负载的部署、保护工作负载的通信方式以及工作负载对其他工作负载的影响。

备注

1. Borg 是谷歌的集群管理系统，用于大规模的调度和运行工作负载。Borg 是谷歌第一个统一容器管理系统，是 Kubernetes 的灵感来源。
2. “左移”是指在软件开发生命周期的早期以前执行相关步骤，可能包括代码、构建、测试、验证和部署等步骤。生命周期图表通常是从左到右绘制，所以“左”表示在较前的步骤。
3. 蓝/绿部署是一种在不影响传入流量的情况下发布工作负载更改内容的方法，以便最终用户在访问时不会遭遇停机。
4. 为了更好地理解流量是如何在谷歌的基础架构中从 GFE 路由到服务的，请参阅《传输加密》白皮书中的“流量路由方式”部分。
5. Borgmaster 是 Borg 的集中控制器。它负责管理作业的调度，并与正在运行的作业通信。

奇安信身份安全实验室出品

谷歌基础架构安全设计概述——谷歌云白皮书

编者按：

在谷歌近期公开的BeyondProd项目白皮书（《谷歌 BeyondProd：一种新的云原生安全方法》）中，详细介绍了谷歌的众多基础架构是如何在云原生（cloud-native）架构中进行协同工作来保护工作负载（workload）的。作为全球最大的网络服务商之一，谷歌基础架构的重要性及对其安全性保障的必要性不言而喻。谷歌在成立初期就一直致力于提升其基础架构全方面的安全能力，在BeyondProd白皮书中，谷歌也特别提到可参考其在2017年发布的这篇《安全基础架构设计白皮书》来了解其在基础架构中是如何设计基础架构安全的。在此我们也特别翻译了本篇谷歌云白皮书，供业界同仁参考、交流。

本文所包含的内容截止至2017年1月是正确的，代表了截止至本文撰写时的现状。随着谷歌不断提高对用户的安全防护，安全策略和系统可能会发生变化。

谷歌基础架构安全设计概述——谷歌云白皮书

面向CIO的概要

- 谷歌的技术基础架构覆盖全球，可为谷歌信息处理的整个生命周期提供安全保障。该基础架构提供服务安全部署、在保护最终用户隐私的前提下进行数据安全存储、保障服务之间安全通信、确保客户通过互联网进行安全和私密的进行通信，以及使管理员能够安全地进行操作。
- 谷歌利用这一基础架构来构建其互联网服务，包括个人用户服务如搜索、Gmail和谷歌相册等，以及企业服务如G Suite和谷歌云平台等。
- 基础架构的安全性是分层逐步设计实现，从数据中心的物理安全开始，再到构成基础架构基础的硬件和软件的安全，最后到支持运营安全的技术约束和流程。
- 谷歌为保护其基础架构安全性投入巨大，拥有数百名致力于安全和隐私的工程师，其中不乏许多公认的行业权威人士。

奇安信身份安全实验室

简介

本文概述了如何将安全性设计到谷歌的技术基础架构中。这一全球规模的基础架构旨在为谷歌的整个信息处理生命周期提供安全保障。该基础架构提供安全的服务安全部署、在保护最终用户隐私的前提下进行数据安全存储、保障服务之间的安全通信、确保客户通过互联网进行安全和私密的进行通信，以及使管理员能够安全地的进行操作。

谷歌通过这一基础架构来构建其互联网服务，包括个人用户服务如搜索、Gmail 和谷歌相册等，和企业服务如 G Suite 和谷歌云平台。

本文将分层级逐步描述该基础架构的安全设计，首先是数据中心的物理安全，然后是构成基础架构基础的硬件和软件安全，最后将描述支持运营安全的技术约束和流程。

Google Infrastructure Security Layers

Operational Security
Intrusion Detection
Reducing Insider Risk
Safe Employee Devices & Credentials
Safe Software Development

Internet Communication
Google Front End
DoS Protection

Storage Services
Encryption at rest
Deletion of Data

User Identity
Authentication
Login Abuse Protection

Service Deployment
Access Management of End User Data
Encryption of Inter-Service Communication
Inter-Service Access Management
Service Identity, Integrity, Isolation

Hardware Infrastructure
Secure Boot Stack and Machine Identity
Hardware Design and Provenance
Security of Physical Premises

图 1. 谷歌基础架构安全层：从位于底层的硬件基础架构到位于顶层的运营安全的各个安全层。文中详细介绍了每层的内容。

© 2020 奇安信集团 保留所有权利

底层基础架构安全

本节将描述如何保护基础架构的最底层安全，从物理位置到数据中心的专用硬件，再到运行在每台机器上底层软件堆栈。

物理位置安全

谷歌设计并建立了自己的数据中心，其中包括多层物理安全保护。仅有极少数谷歌员工具有访问这些数据中心的权限。我们使用多个物理安全层来保护数据中心所在位置，并使用生物识别、金属检测、摄像头、车辆屏障和基于激光的入侵检测系统等技术。此外，谷歌还在第三方数据中心托管了一些服务器，除了数据中心运营商提供的安全层之外，我们确保有受谷歌控制的物理安全措施。例如，在这些地点，我们可以运行独立的生物识别系统、摄像机和金属探测器。

硬件设计与供应

谷歌数据中心由数千台连接到本地网络的服务器组成。服务器主板和网络设备都由谷歌定制设计。我们会对合作的组件供应商进行审查，并谨慎选择组件，同时与供应商一起审核和验证组件提供的安全属性。我们还设计定制了目前部署在服务器和外设上的硬件安全芯片。这些芯片允许我们在硬件层面安全地识别和验证过合法的谷歌设备。

堆栈启动和机器身份标识安全

谷歌服务器使用各种技术来确保其正在启动正确的软件堆栈。我们对 BIOS、引导加载程序、内核和基本操作系统映像等底层组件使用加密签名。可以在每次启动或更新期间验证这些签名。这些组件全部由谷歌控制、构建和加固。对于每一代新硬件，我们都在不断提高安全性：例如，根据各代服务器设计的不同，我们将启动链的信任建立在可锁定的固件芯片、运行谷歌编写的安全代码的微控制器或上述谷歌设计的安全芯片上。

数据中心中的每台服务器上都有自己的特定身份标识，该标识可以与硬件信任根和机器启动时使用的软件绑定。该身份标识用于验证与机器上底层管理服务之间的 API 调

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

用。

谷歌还开发了自动化系统，以确保服务器上运行最新版本的软件堆栈（包括安全补丁），来检测和诊断硬件和软件问题，并在必要时将机器从服务中删除。

服务部署安全

在介绍完基础硬件和软件的安全性后，现在我们将继续介绍如何确保在基础架构上安全地部署服务。“服务”是指开发人员编写并希望在基础架构上运行的应用二进制文件，例如，Gmail SMTP 服务器、Bigtable 存储服务器、YouTube 视频转码器或运行客户应用上的应用引擎沙箱。为了处理所需规模的工作负载，可能有数千台机器运行同一服务的副本。运行在基础架构上的服务由名为 Borg 的群集编排服务控制。

下面将会讲到，基础架构不会假定在基础架构上运行的服务之间存在信任。换句话说，本质上基础架构就是为了适用多租户模式而设计。

服务身份标识、完整性与隔离

谷歌在应用层使用加密身份认证和授权进行服务间通信。这就提供了高度抽象且细粒度的访问控制机制，无论是管理员还是服务都可以理解。

我们不依赖内部网络分段或防火墙作为主要安全机制，不过在网络的各点还是使用了入站和出站过滤作为一层额外的安全防护，用以防止 IP 欺骗。这种方法也有助于最大限度地提高网络性能和可用性。

在基础架构上运行的每项服务都有一个关联的服务帐户身份标识。为服务提供加密凭据，在服务向其他服务发送或从其他服务接收远程过程调用（RPC）时，可以用这些凭据来证明其身份。客户端使用这些身份标识来确保其正在与正确的目标服务器通信，服务器使用这些身份标识将方法和数据访问限定给指定客户端。

谷歌的源代码存储在中央代码库中，在其中服务的当前和过去版本都可被审计。该基础架构还可以配置为：要求服务的二进制文件由经过特定审查、登记和测试的源代码构建。此类代码审查需要开发者之外的至少一名工程师进行检查和批准，并且系统强制

奇安信身份安全实验室出品

要求对任何系统的代码修改必须得到该系统所有者的批准。这些要求限制了内部人员或攻击者恶意修改源代码的能力，还提供了从服务回溯 到源代码的取证跟踪。

谷歌有多种隔离和沙箱技术，用于保护服务免受运行在同一台机器上的其他服务影响。这些技术包括正常的Linux用户分离、基于语言和内核的沙箱以及硬件虚拟化。总之，我们会为高风险的工作负载使用更多的隔离层；例如，当对用户提供的数据运行复杂的文件格式转换器时，或者当为谷歌应用引擎（Google App Engine）或谷歌计算引擎（Google Compute Engine）等产品运行用户提供的代码时。作为额外的安全防线，特别敏感的服务（如集群编排服务和一些密钥管理服务）将只在专用机器上运行。

服务间访问管理

服务的所有者可以使用基础架构提供的访问管理功能来确切地指定哪些服务可以与其通信。例如，一项服务可能希望仅向列入白名单的其他服务提供一些API。可以使用列了允许的服务账号身份标识的白名单配置该服务，然后基础架构会自动强制执行此访问限制。

访问服务的谷歌工程师也会被授予个人身份标识，因此可以对服务进行类似的配置，以允许或拒绝他们的访问。所有这些类型的身份标识（机器、服务和员工）都位于基础架构维护的全局名称空间中。最终用户的身份标识将分开处理（后文将详细展开）。

谷歌基础架构为这些内部身份标识提供了丰富的身份管理工作流系统，包括审批链、日志记录和通知。例如，可以通过允许两方控制的系统将这些身份标识分配给访问控制组，其中一名工程师可以提议对一个组进行更改，而提议必须得到另一名工程师（同时也是该组的管理员）的批准。此系统允许安全的访问管理进程扩展到基础架构上运行的数千项服务。

除了自动化的API级的访问控制机制外，基础架构还允许服务从中心ACL和组数据库中读取数据，以便其可以在必要时执行自定义的细粒度访问控制。

奇安信集团安全研究院出品

服务间通信加密

在前面部分讨论的 RPC 身份验证和授权功能之外，基础架构还通过加密为网络上的 RPC 数据提供隐私性和完整性。为了向 HTTP 等其他应用层协议提供这些安全收益，将它们封装在基础架构 RPC 机制中。这实际上会提供应用层隔离，并消除对网络路径安全性的依赖。即使网络被窃听或网络设备被破坏，经加密的服务间通信仍可保持安全。

服务可以为每个基础架构 RPC 配置所需的加密保护级别（例如，对数据中心内的低价值数据，可仅配置完整性级别保护）。为了防止高级攻击者窃听我们私有广域网链路，基础架构会自动加密流经数据中心之间广域网的所有基础架构 RPC 流量，而无需服务本身进行任何具体配置。通过硬件加密加速器的部署，可以将此默认加密扩展到数据中心内的所有基础架构 RPC 流量。

最终用户数据的访问管理

谷歌服务一般来说就是为服务最终用户而编写。例如，最终用户可以将他们的电子邮件存储在 Gmail 上。最终用户与 Gmail 等应用的交互会调用基础架构中的其他服务。例如，Gmail 服务可以调用“联系人”这项服务的 API 来访问最终用户的通讯录。

在前一节中可以看到“联系人”服务可以配置为只允许来自 Gmail 服务（或“联系人”服务允许的任何其他特定服务）的 RPC 请求。

不过，这仍然是一组非常宽泛的权限。在该权限范围内，Gmail 服务可以随时请求任何用户的联系人。

由于 Gmail 服务代表特定的最终用户向“联系人”服务发出 RPC 请求，因此基础架构赋予 Gmail 服务一项功能，使其可以将“最终用户权限票据”作为 RPC 的一部分提交。此票据可证明 Gmail 服务当前正在代表该特定最终用户的发起请求。这使“联系人”服务确保只返回票据中指定的最终用户的数据。

基础架构提供一项中央用户身份识别服务来签发“最终用户许可票据”。最终用户登录时由中央身份服务验证用户身份并为用户的客户端设备颁发用户凭据，如 cookie 或 OAuth 令牌。从客户端设备到谷歌发出的任何后续请求都需要提供该用户凭据。

奇安信身份安全实验室出品

当服务接收到最终用户凭据时，它会将凭据传递给中央身份识别服务进行验证。如果最终用户凭据验证正确无误，则中央身份识别服务会返回短期有效的“最终用户许可票据”用于与请求相关的RPC。在这个例子中，获得“最终用户许可票据”的服务是Gmail服务，它将把票据传递给“联系人”服务。之后，对于任何级联调用，调用服务都可以将“最终用户权限票证”作为RPC调用的一部分传递给被调用服务。

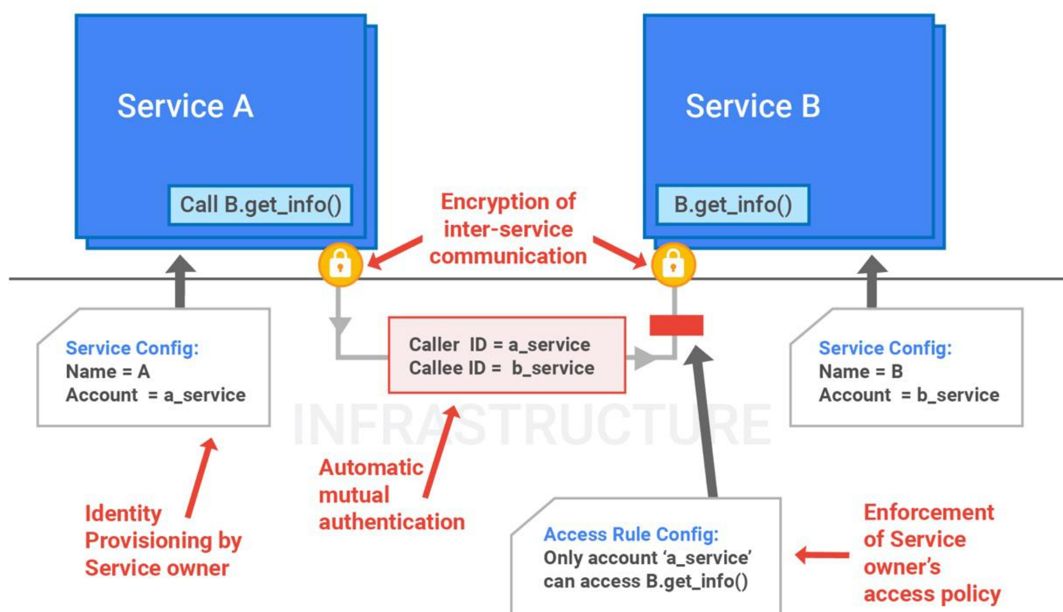


图 2. 服务身份标识和访问管理：基础架构提供服务身份标识、自动化的双向身份验证、加密的服务间通信以及执行由服务所有者定义的访问策略。

数据存储安全

前文已经介绍了如何安全地部署服务。接下来开始讨论如何在基础架构上实现安全的数据存储。

静态加密

谷歌的基础架构提供多种存储服务，如Bigtable和Spanner，以及中央密钥管理服务。谷歌的大多数应用通过这些存储服务间接访问物理存储。存储服务可以配置为在数据写入物理存储之前使用中央密钥管理服务中的密钥对数据进行加密。此密钥管理服务

© 2020 奇安信集团 保留所有权利

支持自动密钥轮换，提供大量审计日志，并与前面提到的最终用户许可票据集成，以将密钥与特定的最终用户关联。

在应用层执行加密可使基础架构将自身与底层存储的潜在威胁（如恶意磁盘固件）隔离开。也就是说，基础架构还可以实施额外的保护层。我们在硬盘和固态硬盘中启用硬件加密支持，并在每个硬盘的生命周期中仔细跟踪每个硬盘。对于停用的加密存储设备，先通过多步骤流程（包括两次独立验证）清空其内容，再撤离我们的管控范围。未通过此擦除过程的设备会在本地进行物理销毁（如粉碎）。

删除数据

谷歌数据删除流程的第一步通常是将特定数据标记为“已安排删除”，而不是一开始就做彻底移除。这使得我们可以恢复无意删除的数据（无论是由客户发起，还是因内部缺陷或处理错误而造成的删除）。在被标记为“已安排删除”后，将根据服务的专用策略来删除数据。

当最终用户删除其整个帐户时，基础架构将通知处理最终用户数据的服务该帐户已被删除。然后，服务可以安排对与已删除的最终用户帐户关联的数据进行删除。此功能使服务的开发人员能够轻松实现最终用户控制。

互联网通信安全

前文介绍了如何在基础架构上保护服务。本节将介绍如何保护互联网和这些服务之间的通信安全。

如前所述，基础架构由大量物理机组成，这些物理机通过局域网和广域网互连，服务间通信的安全性不依赖于网络的安全性。不过，我们还是将基础架构从互联网隔离到私有 IP 空间，而只将一小部分机器直接暴露于外部互联网流量中，这样就可以更容易实现额外的保护，例如防止拒绝服务（DoS）攻击。

奇安信身份安全实验室出品

谷歌前端服务

当一项服务想要在互联网上可用时,它可以向名为谷歌前端(Google Front End, GFE)的基础架构服务进行注册。通过使用正确的证书并遵循最佳实践(例如支持完美的前向安全性),谷歌前端服务(GFE)可确保终止所有 TLS 连接。此外,GFE 还应用了拒绝服务攻击(DoS)防护(稍后我们将详细讨论)。然后,GFE 使用前面讨论的 RPC 安全协议转发服务请求。

实际上,任何选择对外发布的内部服务都使用 GFE 作为智能反向代理前端。该前端提供公开 IP 托管公开的 DNS 名称、防护拒绝服务(DoS)攻击以及终止 TLS 连接。请注意,GFE 与任何其他服务一样在基础架构上运行,因此能够根据入站请求量进行调节。

拒绝服务(DoS)防护

规模庞大的谷歌基础架构可以轻而易举地抵抗许多拒绝服务 DoS 攻击。我们有多层级 DoS 防护,可进一步降低使用 GFE 的服务受到 DoS 攻击影响的风险。

在骨干网向其中一个数据中心提供外部连接后,它将经过几层软硬件负载平衡。这些负载均衡向运行在基础架构上的中央 DoS 服务报告有关入站流量的信息。当中央 DoS 服务检测到 DoS 攻击时,可以配置负载均衡,丢弃或限制与该攻击相关的流量。

在下一层,GFE 实例还向中央 DoS 服务报告它们正在接收的请求的信息,包括负载平衡没有的应用层信息。然后,中央 DoS 服务还可以配置 GFE 实例以降低或限制攻击流量。

用户身份认证

在 DoS 防护后,下一层防御来自我们的中央身份识别服务。此服务通常以谷歌登录页面的形式显示给最终用户。除了要求提供简单的用户名和密码外,该服务还根据风险因素智能地要求用户提供其他信息,例如用户过去是否使用同一设备或在相同位置登录过。在对用户进行身份认证后,身份识别服务会签发可用于后续调用的凭据,如 cookies 和 OAuth 令牌。

奇安信集团安全实验室出品

用户还可以选择在登录时使用第二因素身份认证，如 OTP 或防钓鱼安全密钥。为了使谷歌以外的其他组织机构也能使用这些服务，我们通过 FIDO 联盟与多家设备供应商合作开发了通用第二因素（U2F）开放标准。这些设备现已上市，其他主流 Web 服务也同步实现了 U2F 支持。

运营安全

到目前为止，我们已经介绍了如何将安全性设计到基础架构中，并且还介绍了一些安全运营机制，例如对 RPC 的访问控制。

接下来将介绍如何安全地运营基础架构：安全地创建基础架构软件，保护员工的机器和凭证，防御来自内部和外部操作者对基础架构的威胁。

安全的软件开发

除了前面介绍的中央源代码控制和双方审核功能外，我们还提供了一些可阻止开发人员引入某些特定类别的安全错误库。例如，我们有消除 Web 应用中 XSS 漏洞的库和框架。我们还拥有自动检测安全错误的自动化工具，包括模糊测试工具、静态分析工具和 Web 安全扫描器。

作为检查的最后一项，通过人工安全审核的方式，审核范围覆盖从对较低风险的功能进行快速分类，到对最高风险的功能在设计和实施上进行深入审核。执行这些审核的团队由 Web 安全、加密和操作系统安全领域的专家组成。此外，此类审核还可能催生出新的安全库功能和新的模糊测试工具，可用于未来的其他产品。

此外，谷歌还实施了漏洞奖励计划，为任何能发现我们基础架构或应用漏洞并告知我们的人员提供奖励。目前谷歌已经发放了数百万美元的奖励。

谷歌还投入大量精力查找我们使用的所有开源软件中的零日漏洞和其他安全问题，并上报这些问题。例如，谷歌发现了 OpenSSL 心脏滴血漏洞，并且针对 Linux KVM hypervisor，谷歌是提交 CVE 和安全漏洞修复解决方案最多的一家公司。

奇安信身份安全实验室出品

确保员工设备和凭据的安全

谷歌投入大量成本用于保护员工的设备和凭据免遭破解，并会监控相关活动以发现潜在的损害或内部人员的非法行为。这部分投资是我们用于确保基础架构安全运行的投资中的关键部分。

谷歌员工一直饱受高级网络钓鱼攻击的威胁。为了防范这种威胁，我们要求员工账号强制使用兼容U2F的安全密钥,替换了可能被钓鱼攻击的OTP第二因素进行身份认证。

我们投入大量成本来管控员工用来运行基础架构的客户端设备。谷歌需确保这些客户端设备的操作系统镜像具有最新的安全补丁，并控制可安装的应用。此外，我们配备了相应系统来扫描用户安装的应用、下载内容、浏览器扩展和从web上浏览内容，以确保其适合企业客户端。

是否在公司局域网上不是我们用来判断是否授予访问权限的主要机制。我们使用的是应用级访问管理控制机制，这使我们可以仅向来自正确的受控设备、预期的网络和地理位置的特定用户公开内部应用。(要了解详情,请参阅“BeyondCorp”相关阅读材料。)

降低内部风险

针对拥有基础架构管理员权限的员工行为，我们采取了积极主动地限制和监控，并通过自动化手段使得这些限制与监控更安全、更可控，不断努力消除特定任务对于特权访问的需求。这包括要求某些操作得到双方批准方可执行，并引入有限的API，允许在不公开敏感信息的情况下进行调试。

谷歌员工对最终用户信息的访问通过底层基础架构钩子进行记录。谷歌的安全团队会主动监控访问模式并调查异常事件。

入侵检测

谷歌拥有先进的数据处理管道，这些管道集成了各个设备上基于主机的信号、来自基础架构中各个监控点的基于网络的信号以及基础架构服务的信号。在管道上建立的规则和机器智能为运营安全工程师提供可能发生的事故的告警。我们的调查和事件响应团

奇安信身份安全实验室出品

队一年 365 天，每天 24 小时对这些潜在事件进行分类、调查和响应。我们还会进行红队演习，用以衡量和改善我们检测和响应机制的有效性。

Google 云平台（GCP）安全

本节将重点介绍谷歌的公有云基础架构谷歌云平台（Google Cloud Platform，GCP）如何从底层基础架构的安全性中获益。在本节中，我们将以谷歌计算引擎（Google Compute Engine，GCE）为例，详细描述我们在基础架构之上构建的、针对特定服务的安全性改进。

GCE 使客户能够在谷歌的基础架构上运行自己的虚拟机。GCE 的实现涉及到若干逻辑组件，最显著的是管理控制平面和虚拟机本身。

管理控制平面暴露外部 API 和编排虚拟机创建和迁移等任务。和其他各种服务一样它运行在基础架构上，因此自动获得基础的完整性功能，例如安全启动链。各个服务在不同的内部服务帐户下运行，因此每个服务只能被授予它与控制平面的其他服务进行远程过程调用（RPC）所需的权限。如前所述，所有这些服务的代码都存储在谷歌的中央源代码存储库中，并且在这些代码和最终部署的二进制文件之间有审计跟踪。

GCE 控制平面通过 GFE 公开其 API，因此它可以利用了基础架构提供的安全特性，如拒绝服务（DoS）保护和集中管理的 SSL/TLS 支持。通过选择使用构建在 GFE 上的可选的谷歌云负载均衡器服务，客户可以为运行在 GCE 的虚拟机（VM）上的应用获得类似的保护，也可以减轻许多类型的 DoS 攻击。

GCE 控制平面 API 的最终用户身份认证是通过谷歌的集中式身份服务完成的，该服务提供了诸如劫持检测等安全功能。授权是使用中央 Cloud IAM 服务完成的。

控制平面的网络流量，无论是从 GFE 到它后面的第一个服务，还是其他控制平面服务之间的网络流量，都由基础架构自动认证，并在它从一个数据中心传输到另一个数据中心时加密。此外，该基础架构还配置为对数据中心内部的一些控制平面流量进行加密。

每个虚拟机（VM）都与关联的虚拟机管理器（VMM）服务实例一起运行。基础架构为这些服务提供了两个标识。一个标识由 VMM 服务实例用于自己的调用，一个标识用于

奇安信安全实验室出品

© 2020 奇安信集团 保留所有权利

VMM 代表客户的 VM 进行的调用。这样我们就可以进一步细分对来自 VMM 调用中的植入的信任。

GCE 永久磁盘存储时采用受中央基础架构密钥管理系统保护的密钥进行过加密，因此密钥就可以自动轮转并对密钥访问集中审计。

如今客户有了更多选择，可以选择在不加密的情况下从其 VM 向其他 VM 或互联网发送流量，也可以选择对该流量进行所需加密。我们已经为客户的 VM 到 VM 流量在广域网中遍历的每一跳提供自动加密。目前，基础架构内所有的控制平台广域网流量已经被加密。未来，我们计划利用前面讨论的硬件加速网络加密来同样加密数据中心内的 VM 之间的局域网流量。

提供给 VM 的隔离是在硬件虚拟化的基础上使用开源 KVM 堆栈实现。通过将一些控制措施和硬件仿真堆栈移动到内核外的非特权进程中，我们进一步加固了 KVM 的特定实现。我们还使用模糊化、静态分析和人工代码审查等技术对 KVM 的核心进行了广泛的测试。如前所述，最近公开并已上传至 KVM 的大部分漏洞是由谷歌披露的。

最后，我们的运营安全控制是确保数据访问遵循我们策略的关键部分。作为谷歌云平台的一部分，GCE 对客户数据的使用遵循 GCP 对客户数据的使用策略，即除非为客户提供的相关服务需要，谷歌不会访问或使用客户数据。

结论

我们已经描述了谷歌的基础架构是如何在互联网范围安全地构建、部署和操作服务的。这包括 Gmail 等个人用户服务和企业服务。此外，我们的谷歌云服务也建立在同样的基础架构之上。

我们为保护谷歌基础架构的安全性投入巨大，包括数百名致力于安全和隐私的工程师致力于此，其中不乏许多公认的行业权威人士。

正如我们所看到的，基础架构的安全性是分层级设计的，从物理组件和数据中心开始，到硬件来源，然后到安全启动，服务间通信安全，数据存储安全，从因特网访问服务的保护和最后我们为运营安全部署的技术和人员流程。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

补充阅读

有关领域的详细信息，请参阅以下材料：

1. 数据中心的物理安全(https://goo.gl/WYIKGG)
2. 集群管理和编排设计(https://research.google.com/pubs/pub43438.html)
3. 存储加密和面向客户的 GCP 加密功能 (https://cloud.google.com/security/encryption-at-rest/)
4. BigTable 存储服务(https://research.google.com/archive/bigtable.html)
5. Spanner 存储服务 (https://research.google.com/archive/spanner.html)
6. 网络负载均衡体系结构(https://research.google.com/pubs/pub44824.html)
7. 企业安全方法 BeyondCorp(https://research.google.com/pubs/pub43231.html)
8. 用安全密钥和通用 U2F 标准对抗网络钓鱼 (https://research.google.com/pubs/pub45409.html)
9. 关于谷歌漏洞奖励计划的更多信息(https://bughunter.withgoogle.com/)
10. 有关 HTTPs 和 GCP 上其他负载均衡产品的更多信息 (https://cloud.google.com/compute/docs/load-balancing/)
11. 有关 DoS 保护最佳实践的详细信息 (https://cloud.google.com/>les/GCPDDoSprotection-04122016.pdf)
12. 谷歌云平台客户数据使用政策(https://cloud.google.com/terms/)
13. 有关 G Suite 中应用安全性和合规性的更多信息（Gmail、驱动器等 (https://static.googleusercontent.com/media/gsuite.google.com/en//>les/google-apps-security-and-compliance-whitepaper.pdf)

奇安信集团安全实验室出品

NIST 标准《零信任架构》草案 1 全文

一、前言

本文开始介绍 2019 年 9 月发布的 NIST《零信任架构》草案（《NIST.SP.800-207-draft-Zero Trust Architecture》）。其公开评论的时间是 2019 年 9 月 23 日至 2019 年 11 月 22 日。本文档的价值，不言而喻。

其目录如下：

- 摘要
- 1. 介绍
- 2.零信任网络架构
- 3.零信任体系架构的逻辑组件
- 4.部署场景/用例
- 5.与零信任架构相关的威胁
- 6.零信任架构与现有联邦指南
- 7.迁移到零信任架构
- 附录 A：缩略语
- 附录 B：识别 ZTA 当前技术水平的差距

与零信任密切相关的其它重要资料包括：

- 2019 年 4 月，**ACT-IAC（美国技术委员会-工业咨询委员会）**发布的**《零信任网络安全当前趋势》**（《Zero Trust Cybersecurity Current Trends》），参见《网络安全架构|零信任网络安全当前趋势（下）》。上、中、下的整合版可参见：“互联网安全内参”《深度剖析：零信任网络安全当前趋势》。
- 2019 年 7 月，**美国国防部国防创新委员会（DIB，Defense Innovation Board）**发布的 **DIB 零信任架构白皮书**（DIB Zero Trust White Paper）**《零信任安全之路》**（The Road to Zero Trust (Security)），参见《网络安全架构 | 零信任架构正在标准化》的第四节。

说明：除了开篇的背景内容，凡是没有使用“笔者说明：”开头的段落，都基本是按照原文进行翻译的。但是对于有些翻译拿不准或者文字赘述的内容，也会做少量删节。

奇安信行业安全实验室出品

© 2020 奇安信集团 保留所有权利

二、文档摘要信息

1）摘要

零信任（zero trust）是一组不断发展的网络安全范例的术语，它将网络防御从广泛的网络周界转移到仔细关注单个或小组资源。**零信任架构**（ZTA，Zero Trust Architecture）策略是指基于系统的物理或网络位置（即局域网或因特网）不存在授予系统的隐式信任的策略。当需要资源时才授予对数据资源的访问权，并在建立连接之前执行身份验证（用户和设备）。ZTA 是对企业网络趋势的响应，这些趋势包括远程用户和不在企业拥有的网络边界内的基于云的资产。ZTA 的重点是保护资源，而非网络分段，因为网络位置不再被视为资源安全态势的主要组成部分。本文包含了 ZTA 的抽象定义，并给出了 ZTA 可以改善企业整体 IT 安全状况的一般部署模型和用例。

2）致谢

本文件是多个联邦机构合作的产物，由联邦首席信息官委员会监督。架构小组负责本文档的开发，但有一些特定的人员值得认可。

3）受众

本文档旨在为企业网络架构师描述 ZTA 策略。

该文件旨在帮助理解民用非保密系统的 ZTA，并提供将 ZTA 概念迁移和部署到企业网络的路线图。

机构网络安全经理、网络管理员、经理也可以从本文档中了解 ZTA。

本文档的目的不是针对 ZTA 的单一部署计划，因为企业将拥有需要保护的独特业务用例和数据资产。从对组织的业务和数据有一个坚实的了解开始，这将导致一个强大的零信任方法。

笔者说明：本文档的核心对象是为“网络架构师”准备的，而非“安全架构师”。这应该是“内生安全”和“安全左移”的应有之义。要想真正贯彻零信任思想，就需要了解组织的网络、业务和数据，这些都是与组织对象密切相关的。笔者经常会有个疑问：是该做安全的人了解业务，还是该做业务的人了解安全。从“本文档旨在为企业网络架构师描述 ZTA 策略”这句话看，本文档的作者，甚至联邦首席信息官们，更加倾向于认为：首先应该是做业务的人了解安全。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

4）审阅者注意事项

本特别出版物的目的,是开发一套技术中立的使用ZTA策略的网络基础设施的术语、定义和逻辑组件。本文档不提供如何在企业中部署零信任组件的具体指南或建议。

三、介绍

典型的企业网络基础设施变得越来越复杂。单个企业可以运行多个内部网络、具有自己的本地基础设施的远程办公室、远程和/或移动个人，以及云服务。这种复杂性超过了基于周界的网络安全的传统方法，因为企业没有单一的、易于识别的周界。

这种复杂的企业已经导致了一种新的企业网络安全规划方法，称为**零信任架构（ZTA）**。ZTA方法主要侧重于数据保护，但可以扩展到包括所有企业资产。ZTA假设网络是不怀好意的，并且企业拥有的网络基础设施与任何非企业拥有的网络相比，并没有不同或更加安全。在这种新的范式中，企业必须不断地分析和评估其内部资产和业务功能的风险，然后制定保护措施来缓解这些风险。在ZTA中，这些保护通常涉及最小化对资源的访问，只允许那些被验证为确有需要者的访问，并持续验证每个访问请求的身份和安全状态。

本出版物提供了ZTA的定义、逻辑组件、可能的部署场景和威胁。它还为希望迁移到以ZTA为中心的网络基础设施的组织，提供了一个总体路线图，并讨论了可能影响或确实影响零信任架构的相关联邦政策。

ZTA不是单一的网络架构，而是一套网络基础设施设计和运行的指导原则，可以用来改善任何密级或敏感级别的安全态势。向ZTA过渡是一段旅程。也就是说，现在许多组织的企业基础设施中已经有了ZTA的元素。组织应该逐步实现零信任原则、流程变更和保护其数据资产和业务功能的技术解决方案。在此期间，大多数企业基础设施将以**零信任/遗留模式**混合运行，同时继续投资于正在进行的IT现代化计划和改进的组织业务流程。

组织需要实施有效的信息安全和弹性实践，才能使零信任有效。当与现有的网络安全政策和指南、身份和访问管理、持续监测、通用网络安全相结合时，ZTA能够使用管理风险的方法增强组织的安全姿态，并保护共同威胁。

1）背景

自“零信任”这个词出现之前，零信任的概念就一直存在于网络安全中。Jericho论坛的工作公开了基于网络位置限制隐式信任的思想和依赖静态防御的限制[JERICHO]。去边界化的概念发展并改进为一个更大的概念，称为零信任。后来，Jon Kindervag在

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

Forrester（现在 Palo Alto Networks）创立了“零信任”一词。这项工作包括关键概念和零信任网络架构模型，该模型改进了在 Jericho 论坛上讨论的概念。

十多年来，美国联邦机构在许多方面一直在转向基于零信任原则的网络安全。联邦机构一直在推进相关能力建设和政策，从《联邦信息安全管理法》（FISMA）开始，然后是风险管理框架（RMF）、联邦身份、凭证和访问管理（FICAM）、可信互联网连接（TIC）、持续诊断和缓解（CDM）计划。所有这些计划都旨在限制授权方的数据和资源访问。在这些计划启动时，受到了信息系统技术能力的限制。安全策略基本上是静态的，并在企业可以控制的大“瓶颈”上执行，以获得最佳效果。随着技术的成熟，以动态和细粒度的方式持续分析和评估访问请求，成为可能。

2）本文件的结构

文档的其余部分如下：

- 第 2 节：定义 ZTA 并列出设计 ZTA 企业网络时的一些网络假设。本节还包括 ZTA 设计原则的列表。

•第 3 节：描述 ZTA 的逻辑组件或构建模块。独特的实现可能以不同的方式组合 ZTA 组件，但提供相同的逻辑功能。

•第 4 节：列出一些可能的用例，其中 ZTA 可使企业网络更加安全，更不容易被攻击利用。这包括拥有远程员工、云服务、客户网络等的企业场景。

•第 5 节：讨论了使用 ZTA 策略的企业面临的威胁。其中许多威胁与传统架构的网络相似，但可能需要不同的缓解技术。

•第 6 节：讨论 ZTA 原则如何适合和/或补充了联邦机构现有的指南。

•第 7 节：提出企业（如联邦机构）向 ZTA 过渡的起点。这包括描述在 ZTA 原则指导下规划和部署应用程序和网络基础设施所需的一般步骤。

四、零信任网络架构

零信任体系架构是一种端到端的网络/数据安全方法，包括身份、凭证、访问管理、操作、终端、宿主环境和互联基础设施。零信任是一种侧重于数据保护的架构方法。初

奇安信身份安全实验室出品

始的重点应该是将资源访问限制在那些“需要知道”的人身上。传统上，机构（和一般的企业网络）专注于边界防御，授权用户可以广泛地访问资源。因此，网络内未经授权的横向移动一直是政府机构面临的最大挑战之一。可信 Internet 连接（TIC）和机构边界防火墙提供了强大的 Internet 网关。这有助于阻止来自 Internet 的攻击者，但 TIC 和边界防火墙在检测和阻止来自网络内部的攻击方面用处不大。

一种可用的 ZTA 定义如下：

零信任架构（ZTA）提供了一个概念、思路和组件关系（架构）的集合，旨在消除在信息系统和服务中实施精确访问决策的不确定性。

此定义聚焦于问题的关键，即消除对数据和服务的非授权访问，以及使访问控制的实施尽可能精细。也就是说，授权和批准的主体（用户/计算机）可以访问数据，但不包括所有其他主体（即攻击者）。进一步，"资源"一词可以代替"数据"，以便 ZTA 与资源访问（例如打印机、计算资源、IoT 执行器等）有关，而不仅仅是数据访问。

为了减少不确定性（因为它们不能完全消除），重点是身份验证、授权和缩小隐含信任区域，同时最大限度地减少网络身份验证机制中的时间延迟。访问规则被限制为最小权限，并尽可能细化。

在图 1 中，用户或计算机需要访问企业资源。通过策略决策点（PDP）和相应的策略执行点（PEP）授予访问权限。

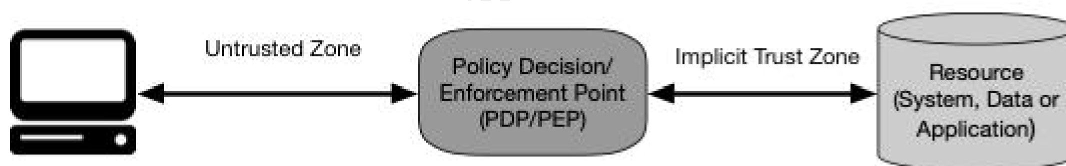


图 1：零信任访问

系统必须确保用户"可信"且请求有效。PDP/PEP 会传递恰当的判断，以允许主体访问资源。这意味着零信任适用于两个基本领域：身份验证和授权。系统能否消除对用户真实身份的足够怀疑？用户在访问请求中是否合理？用于请求的设备是否值得信任？总体而言，企业需要为资源访问制定基于风险的策略，并建立一个系统来确保正确执行这些策略。这意味着企业不应依赖于隐含的可信性，而隐含可信性是指：如果用户满足基本身份验证级别（即登录到系统），则假定所有资源请求都同样有效。

“隐含信任区”表示一个区域，其中所有实体都至少被信任到最后一个 PDP/PEP 网关的级别。例如，考虑机场的乘客筛选模型。所有乘客通过机场安检点（PDP/PEP）进入登机门。乘客可以在候机区内闲逛，所有乘客都有一个共同的信任级别。在这个模型中，隐含信任区域是候机区。

PDP/PEP 应用一组公共的控制，使得检查点之后的所有通信流量都具有公共信任级

© 2020 奇安信集团 保留所有权利

别。PDP/PEP 不能在流量中应用超出其位置的策略。为了使 PDP/PEP 尽可能细致，隐含信任区必须尽可能小。

零信任架构提供了技术和能力，以允许 PDP/PEP 更接近资源。其思想是对网络中从参与者（或应用程序）到数据的每个流进行身份验证和授权。

1）零信任架构的原则

关于 ZTN/ZTA 的许多定义和讨论，都强调从方程式中去掉边界防御（如防火墙等）的概念。然而，大多数人仍然以某种方式定义自己与边界的关系（例如微分段或微边界）。以下是根据应引入的基本原则而不是排除的基本原则来定义 ZTA 的尝试。

零信任架构的设计和部署遵循以下基本原则：

1. **所有数据源和计算服务都被视为资源。**网络可以由几种不同类别的设备组成。网络可能还具有占用空间小的设备，这些设备将数据发送到聚合器/存储，还有将指令发送到执行器的系统等。此外，如果允许个人拥有的设备访问企业拥有的资源，则企业可以决定将其归类为资源。

2. **无论网络位置如何，所有通信都是安全的。**网络位置并不意味着信任。来自位于企业自有网络基础设施上的系统的访问请求（例如，在边界内）必须满足与来自任何其他非企业自有网络的访问请求和通信相同的安全要求。换言之，不应对位于企业自有网络基础设施上的设备自动授予任何信任。所有通信应以安全的方式进行（即加密和认证）。

3. **对单个企业资源的访问是基于每个连接授予的。**在授予访问权限之前，将评估请求者的信任。这可能意味着此特定事务只能在“以前某个时间”发生，并且在启动与资源的连接之前可能不会直接发生。但是，对一个资源的身份验证不会自动授予对另一个不同资源的访问权限。

4. **对资源的访问由策略决定，包括用户身份和请求系统的可观察状态，也可能包括其他行为属性。**一个组织通过定义其拥有的资源、其成员是谁、这些成员需要哪些资源访问权，来保护资源。用户身份包括使用的网络账户和企业分配给该账户的任何相关属性。请求系统状态包括设备特征，如已安装的软件版本、网络位置、以前观察到的行为、已安装的凭证等。行为属性包括自动化的用户分析、设备分析、度量到的与已观察到的使用模式的偏差。策略是组织分配给用户、数据资产或应用程序的一组属性。这些属性基于业务流程的需要和可接受的风险水平。资源访问策略可以根据资源/数据的敏感性而变化。最小特权原则被应用以限制可视性和可访问性。

5. **企业确保所有拥有的和关联的系统处于尽可能最安全的状态，并监视系统以确保它们保持尽可能最安全的状态。**实施 ZTA 战略的企业应建立持续诊断和缓解（CDM）计划，以监测系统状态，并根据需要应用补丁/修复程序。被发现为已失陷、易受攻击和/或非企业所有的系统，与那些企业所有或与企业相关的被认为处于最安全状态的系

© 2020 奇安信集团 保留所有权利

统相比，可能会被区别对待（包括拒绝与企业资源的所有连接）。

6. **在允许访问之前，用户身份验证是动态的并且是严格强制实施的**。这是一个不断的访问、扫描和评估威胁、调整、持续验证的循环。实施 ZTA 策略的企业具有用户供应系统（user provisioning system），并使用该系统授权对资源的访问。这包括使用多因子身份验证（MFA）访问某些（或所有）企业资源。根据策略（如基于时间的、请求的新资源、资源修改等）的定义和实施，在用户交互过程中进行持续监视和重新验证，以努力实现安全性、可用性、使用性和成本效率之间的平衡。

上述原则试图尽可能做到技术不可知（technology-agnostic）。例如，“网络 ID”可以包括几个因素，例如用户名/口令、证书、一次性密码或某些其他标识。

2）零信任视角的网络

对于在网络规划和部署中使用 ZTA 的任何组织，都有一些关于网络连接性的基本假设。其中一些假设适用于企业拥有的网络基础设施，另一些适用于非企业拥有的网络基础设施上使用的企业拥有的资源（例如，公共 WiFi）。在实施 ZTA 战略的企业中，网络的开发应遵循上述 ZTA 原则和以下假设。

2.1） 假设由企业拥有的网络基础设施

1. **企业私有网络并不可信**。系统应始终假设企业网络上存在攻击者，通信应该来以安全的方式进行（见上文的原则 2）。这需要对所有连接进行身份验证，对所有通信流量进行加密操作。

2. **网络上的设备可能不归企业所有或不可配置**。访客和/或外包服务可能包括需要网络访问才能履行其职责的非企业所有系统。这还包括自带设备（BYOD）策略，允许企业用户使用非企业拥有的设备访问企业资源。

3. **没有设备是内生可信的**。在连接到企业拥有的资源之前，每个设备都必须认证自己（无论是对资源还是对 PEP）（请参阅上面的原则 6）。与来自非企业拥有设备的相同请求相比，企业拥有设备可以具有启用身份验证并提供更高信任分数（请参阅第 3.2 节）的构件。用户凭证并不足以对企业资源进行设备认证。

2.2）假设非企业所有的网络基础设施

1. **并非所有的企业资源都在企业拥有的基础设施上**。这包括远程用户和云服务。企业必须能够监视、配置和修补任何系统，但任何系统都可能依赖本地（即非企业）网络进行基础的连接和网络服务（如 DNS 等）。

2. **远程企业用户不能信任本地网络连接**。远程用户应该假设本地（即非企业所有）

奇安信身份安全实验室出品

网络是不怀好意的。系统应该假设所有的流量都被监视并可能被修改。所有连接请求都应该经过身份验证，所有通信流量都应该加密（参见上面的 ZTA 原则）。

五、零信任体系架构的逻辑组件

在企业中，构成 ZTA 网络部署的逻辑组件很多。这些组件可以作为场内服务或通过基于云的服务来操作。图 2 中的概念框架模型显示了组件及其相互作用的基本关系。注意，这是显示逻辑组件及其相互作用的理想模型。从图 1 中，**策略判定点**（PDP）被分解为两个逻辑组件：**策略引擎**（PE）和**策略管理器**（PA）（定义如下）。

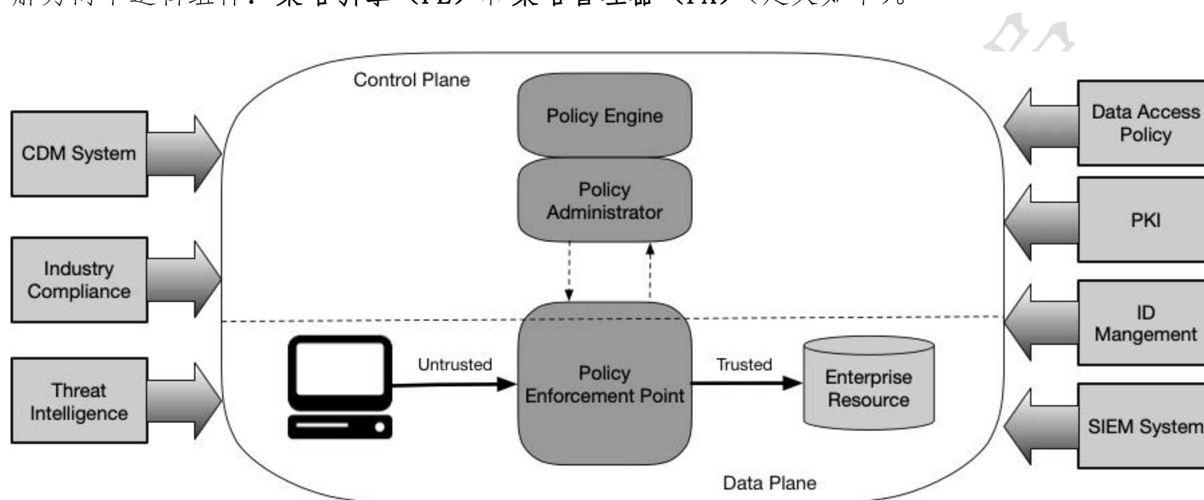


图 2：核心零信任逻辑组件

组件描述：

策略引擎（Policy Engine，PE）：该组件负责最终决定是否授予指定访问主体对资源（访问客体）的访问权限。策略引擎使用企业安全策略以及来自外部源（例如 IP 黑名单、威胁情报服务）的输入作为“信任算法”的输入，以决定授予或拒绝对该资源的访问。策略引擎（PE）与策略管理器（PA）组件配对使用。策略引擎做出（并记录）决策，策略管理器执行决策（批准或拒绝）。

策略管理器（Policy Administrator，PA）：该组件负责建立客户端与资源之间的连接（是逻辑职责，而非物理连接）。它将生成客户端用于访问企业资源的任何身份验证令牌或凭证。它与策略引擎紧密相关，并依赖于其决定最终允许或拒绝连接。实现时可以将策略引擎和策略管理器作为单个服务；这里，它被划分为两个逻辑组件。PA 在创建连接时与策略执行点（PEP）通信。这种通信是通过控制平面完成的。

策略执行点（Policy Enforcement Point，PEP）：此系统负责启用、监视并最终终止主体和企业资源之间的连接。这是 ZTA 中的单个逻辑组件，但也可能分为两个不同的组件：客户端（例如，用户便携式电脑上的代理）和资源端（例如，在资源之前控制访问的网关组件）或充当连接门卫的单个门户组件。

© 2020 奇安信集团 保留所有权利

除了企业中实现 ZTA 策略的核心组件之外，还有几个数据源提供输入和策略规则，以供策略引擎在做出访问决策时使用。这些包括本地数据源和外部（即非企业控制或创建的）数据源。其中包括：

持续诊断和缓解（CDM）系统：该系统收集关于企业系统当前状态的信息，并对配置和软件组件应用已有的更新。企业 CDM 系统向策略引擎提供关于发出访问请求的系统的信息，例如它是否正在运行适当的打过补丁的操作系统和应用程序，或者系统是否存在任何已知的漏洞。

行业合规系统（Industry Compliance System）：该系统确保企业遵守其可能归入的任何监管制度（如 FISMA、HIPAA、PCI-DSS 等）。这包括企业为确保合规性而制定的所有策略规则。

威胁情报源（Threat Intelligence Feed）：该系统提供外部来源的信息，帮助策略引擎做出访问决策。这些可以是从多个外部源获取数据并提供关于新发现的攻击或漏洞的信息的多个服务。这还包括 DNS 黑名单、发现的恶意软件或策略引擎将要拒绝从企业系统访问的命令和控制（C&C）系统。

数据访问策略（Data Access Policies）：这是一组由企业围绕着企业资源而创建的数据访问的属性、规则和策略。这组规则可以在策略引擎中编码，也可以由 PE 动态生成。这些策略是授予对资源的访问权限的起点，因为它们为企业中的参与者和应用程序提供了基本的访问特权。这些角色和访问规则应基于用户角色和组织的任务需求。

企业公钥基础设施（PKI）：此系统负责生成由企业颁发给资源、参与者和应用程序的证书，并将其记录在案。这还包括全球 CA 生态系统和联邦 PKI3，它们可能与企业 PKI 集成，也可能未集成。

身份管理系统（ID Management System）：该系统负责创建、存储和管理企业用户账户和身份记录。该系统包含必要的用户信息（如姓名、电子邮件地址、证书等）和其他企业特征，如角色、访问属性或分配的系统。该系统通常利用其他系统（如上面的 PKI）来处理与用户账户相关联的工件。

安全信息和事件管理（SIEM）系统：聚合系统日志、网络流量、资源授权和其他事件的企业系统，这些事件提供对企业信息系统安全态势的反馈。然后这些数据可被用于优化策略并警告可能对企业系统进行的主动攻击。

1）抽象架构的部署变体

所有这些组件都是逻辑组件。它们不一定是唯一的系统。单个系统可以执行多个逻辑组件的职责，同样，一个逻辑组件可以由多个硬件或软件元素组成，以执行任务。例如，企业 PKI 可以由一个负责为设备颁发证书的组件和另一个用于向最终用户颁发证书的组件组成，但两者都使用从同一企业根证书颁发机构颁发的中间证书。在目前市场上提供的许多 ZTA 网络产品中，PE 和 PA 组件组合在一个服务中。

奇安信身份安全实验室出品

在架构的选定组件的部署上有几个变体，在下面的章节中进行了概述。根据企业网络的建立方式，一个企业中的不同业务流程可以使用多个 ZTA 部署模型。

1.1）基于设备代理/网关的部署

在这个部署模型中，PEP 被分为两个组件，它们位于资源上，或者作为一个组件直接位于资源前面。例如，每个企业发布的系统，都有一个已安装的设备代理来协调连接，而每个资源都有一个组件（即网关）直接放在前面，以便资源只与网关通信，实质上充当了资源的反向代理。网关负责连接到策略管理器（PA），并且只允许由策略管理器（PA）配置的已批准连接（参见图 3）。

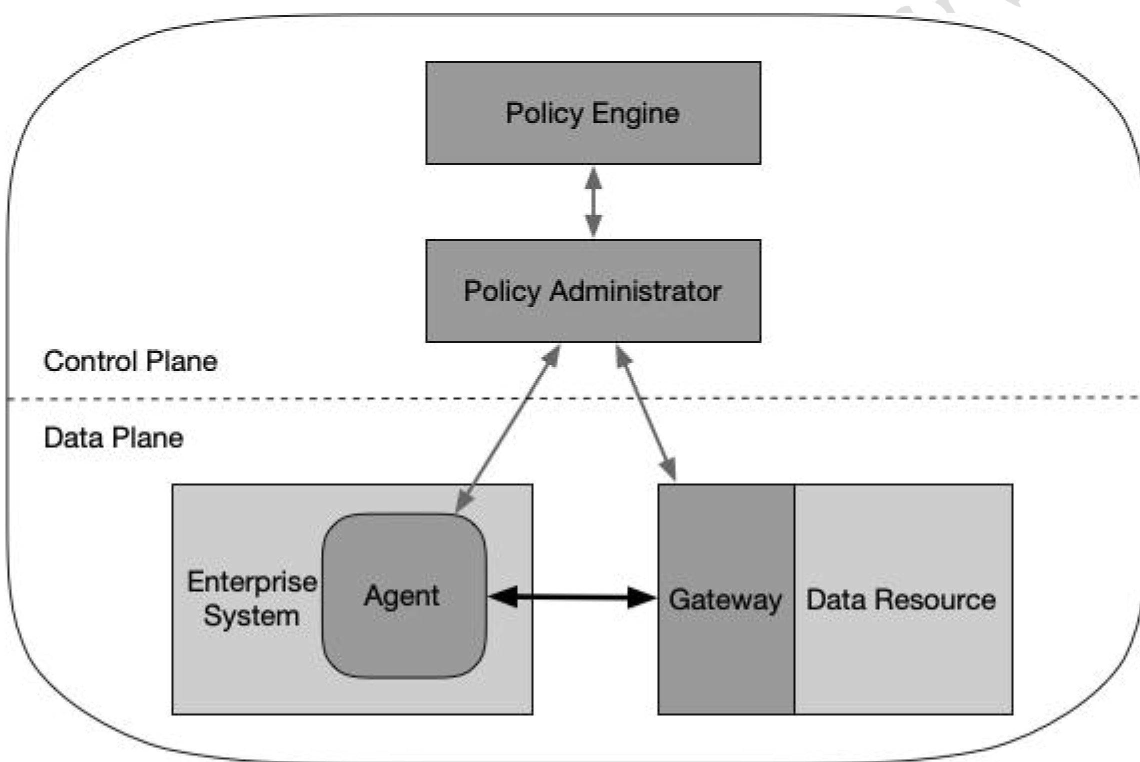


图 3：设备代理/网关模型

在典型的连接场景中，拥有企业发放的笔记本电脑的用户，希望连接到企业资源（例如，HR 应用程序/数据库）。连接请求由本地代理接收，并将连接请求发送给 PA。PA（和 PE）可以是企业本地系统或云托管服务。PA 将请求转发到 PE 进行评估。如果请求被授权，PA 将在设备代理和相关的资源网关（通过控制平面）之间配置通信通道。这可能包括 IP 地址/端口信息、会话密钥或类似的安全构件。然后设备代理和网关连接，加密的应用程序数据流开始。当工作流完成或由于安全事件（例如会话超时、无法重新认证等）被 PA 触发时，设备代理和资源网关之间的连接将终止。

该模型最适合于具有健壮的设备管理程序和可与网关通信的离散资源的企业。对于大量使用云服务的企业，这是云安全联盟（CSA）软件定义周界（SDP）的客户机-服务

© 2020 奇安信集团 保留所有权利

器实现。对于那些不打算允许 BYOD（自带设备）策略的企业来说，这种模式也很好。只能通过设备代理授予访问权限，设备代理可以放置在企业拥有的系统上。

1.2）基于微边界的部署

此部署模型是上述设备代理/网关模型的变体。在这个模型中，网关组件可能不位于系统上或单个资源的前面，而是位于资源飞地（例如，当地数据中心）的边界，如图 4 所示。通常，这些资源服务于单个业务功能，或者可能无法直接与网关通信（例如，没有 API 的遗留数据库系统，不能被用于与网关通信）。此部署模型对于使用基于云的微服务进行业务处理（例如，用户通知、数据库查询或薪资支付）的企业也很有用。在这个模型中，整个私有云位于网关之后。

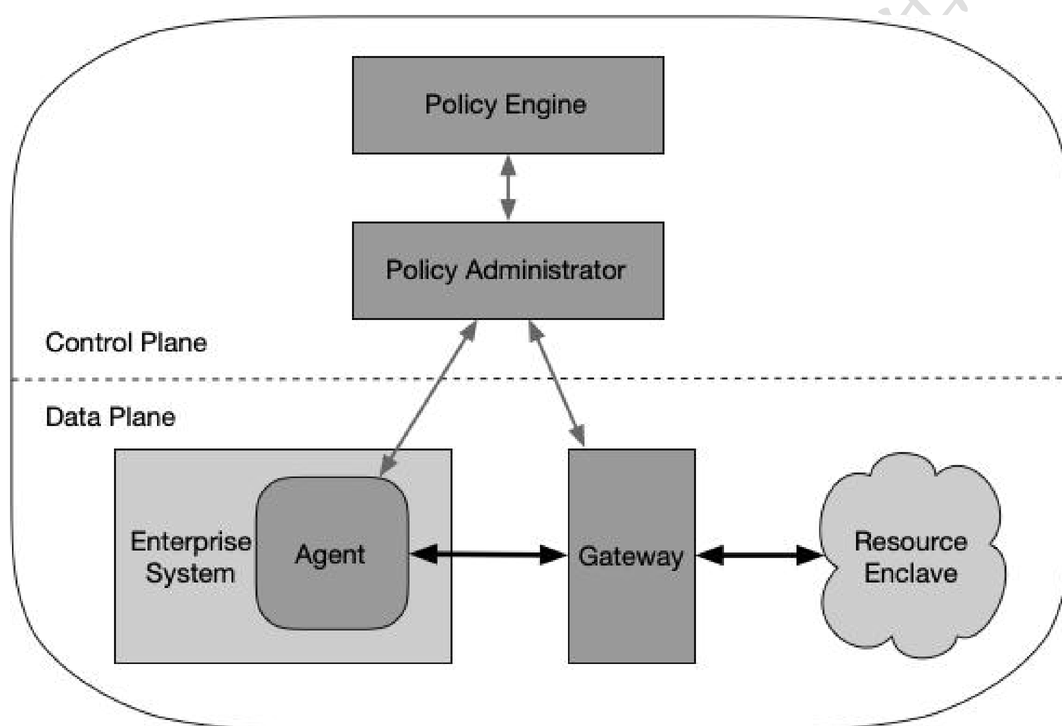


图 4：飞地网关模型

此模型可能与设备代理/网关模型混合。在这样的模型中，企业系统有一个用于连接到微周界网关的设备代理，但是这些连接是使用与基本设备代理/网关模型相同的过程创建的。

此模型对于具有遗留应用程序的企业或无法设置单独网关的场内数据中心非常有用。这样的企业需要有一个健壮的设备管理程序来安装/配置设备代理。缺点是网关保护的是资源集合，而不是单个资源。这是对 ZTA 原则的放松，因为 ZTA 原则要求每种资源都应该有自己的PEP来保护它。这也可能允许了客户端查看它们本无特权访问的资源。

© 2020 奇安信集团 保留所有权利

1.3）基于资源门户的部署

在这个部署模型中，PEP 是一个单独的组件，充当用户请求的网关。网关门户可以是单个资源，也可以是用于单个业务功能的资源集合的微周边。一个例子是进入私有云或包含遗留应用程序的数据中心的网关门户，如图 5 所示。

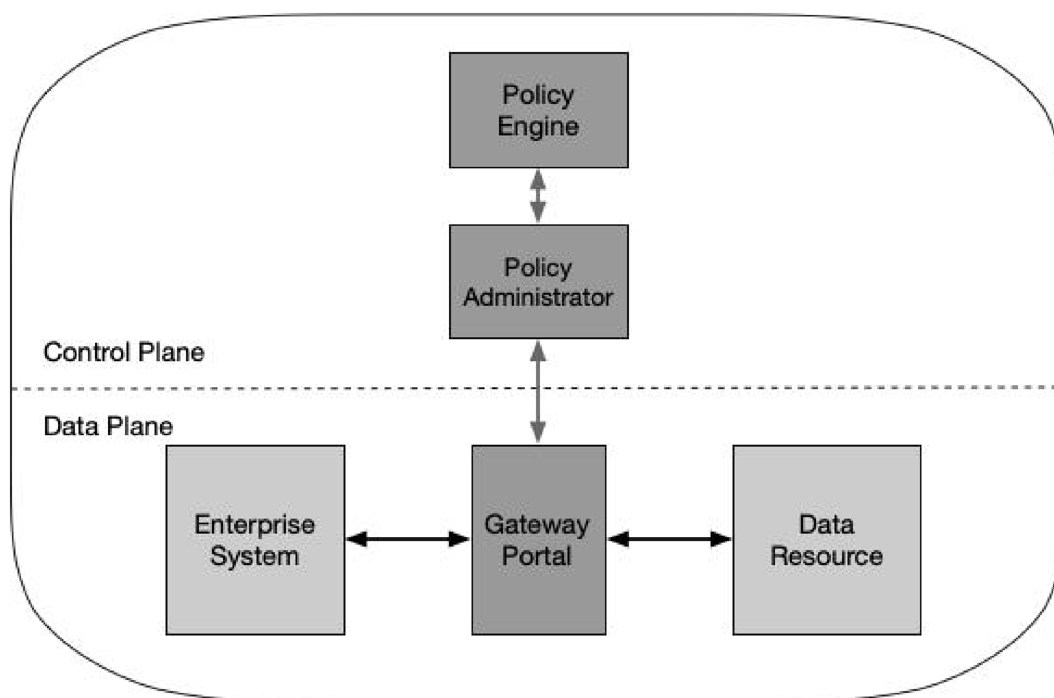


图 5：资源门户模型

与其他模型相比，此模型的主要优点是不需要在所有企业系统上安装软件组件。该模型对于 BYOD 政策和组织间协作项目也更加灵活。企业管理员在使用之前不需要确保每个设备都有适当的设备代理。然而，可以从请求访问的设备推断出有限的信息。它只能扫描和分析连接到 PEP 门户的系统和设备，可能无法持续监视它们是否存在恶意软件和适当的配置。

此模型的主要区别在于没有处理请求的本地代理。此模型允许在客户端系统和 BYOD 策略中具有更大的灵活性，并且可以更容易地对非企业协作者授予资源访问。缺点是，企业可能无法完全看到或控制企业拥有的系统，因为它们只能在连接到门户时看到/扫描这些系统。在这些连接会话之间，这些系统对企业而言可能是不可见的。此模型还允许攻击者发现并尝试访问门户，或尝试对门户进行拒绝服务（DoS）攻击。

1.4）系统应用程序沙箱

代理/网关部署模型的另一个变体是让可信应用程序在系统上隔离运行。这种隔离可以是 VM、容器或其他一些实现，但目标是相同的：保护应用程序不受主机和系统上运

© 2020 奇安信集团 保留所有权利

行的其他应用程序的影响。

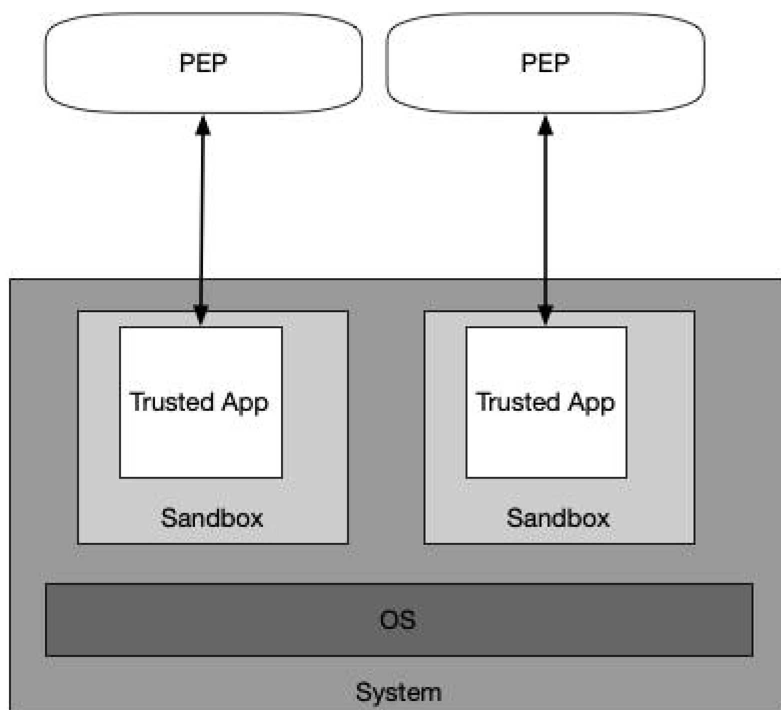


图 6：应用程序沙箱

在上面的图 6 中，用户系统在沙箱中运行可信的应用程序。可信应用程序可以与 PEP 通信以请求对资源的访问，但 PEP 将拒绝来自系统上其他（不可信）应用程序的连接。在这个模型中，PEP 可以是企业本地服务，也可以是云服务。

这种模型变体的主要优点是将单个应用程序与系统的其他部分隔离开来。如果无法扫描系统以检测脆弱性，则可以保护这些单独的沙箱应用程序，使其免受主机系统上潜在的恶意软件感染。这种模式的缺点之一是，企业必须为所有系统维护这些沙盒应用程序，并且可能无法完全看到客户端系统。

2）信任算法

对于部署了 ZTA 的企业，**PE 可以视为大脑，PE 的信任算法是其主要的思维过程。**信任算法是 PE 用来最终授予或拒绝对资源的访问的过程。PE 接受来自多个源的输入：即包含了以下信息的策略数据库——用户、用户属性和角色、历史用户行为模式、威胁情报源、和其他的元数据源的。流程如图 7 所示。

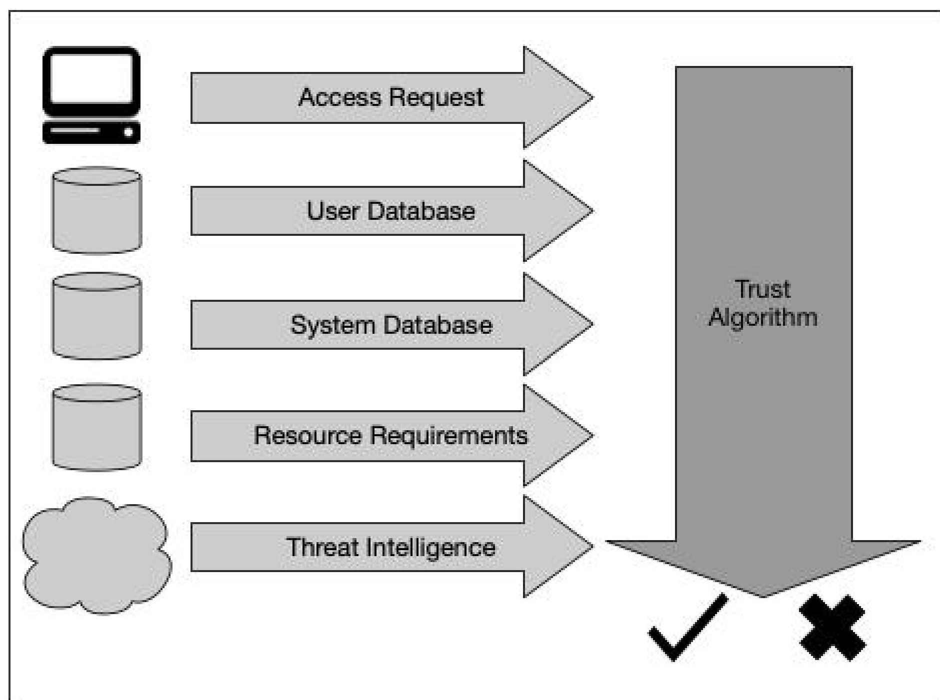


图 7：信任算法的输入

在图中，这些输入可以被分为多个类别，基于它们提供给信任算法的内容。

•**访问请求：**来自应用程序的实际请求。被请求的资源是被使用的主要信息，但也会使用有关请求者的信息。这可能包括操作系统版本、使用的应用程序、修补程序级别。根据系统状态，可能会限制或拒绝对资产的访问。

•**用户标识、属性和权限：**这是请求访问资源的“谁”。这是企业的一组用户（人员和进程）和企业开发的一组用户属性。这些用户和属性构成了资源访问策略的基础。用户身份可以包含以下信息的混合：逻辑身份（例如账户 ID/口令）、生物测定数据（例如指纹、面部识别、虹膜识别、视网膜和气味）和行为特征（例如打字节奏、步态和语音）。身份的属性应被纳入计算信任分数，包括时间和地理因素。授予多个用户的权限集合可以被视为一个角色，但还是应该基于单独个体，将权限分配给一个用户，而不仅仅是因为他们可能适合某个特定角色。这应该被编码并存储在 ID 管理系统和策略数据库中。

•**系统数据库和可观察状态：**系统数据库包含了每一个企业自有系统（在某种程度上是物理的和虚拟的）的已知状态。它会与发生请求的系统的可观察状态相比较。这可以包括操作系统版本、使用的应用程序、位置（网络位置和地理位置）、可信平台模块（TPM）和补丁程序级别。根据系统状态，可能会限制或拒绝对资产的访问。

© 2020 奇安信集团 保留所有权利

•**资源访问要求**：这是对用户 ID 和属性数据库的补充策略集。它定义了访问资源的最低要求。要求可以包括认证器的保障级别，例如多因素认证（MFA）和网络位置（例如，拒绝来自海外 IP 地址的访问）或系统配置请求。这些要求应由数据管理员（即负责数据的人员）和使用数据的负责业务过程的人员（即负责任务/使命的人员）共同制定。

•**威胁情报**：这是一个（或多个）关于 Internet 上运行的一般威胁和活动恶意软件的信息源。它可能包括攻击特征和缓解措施。这是唯一的极少受企业控制但极有可能是一种服务的组件。

关于每个数据源的重要性权重，可以是专有算法，也可以由企业配置。这些权重值可用于反映数据源对企业的重要性。

最终的决策会交给 PA 执行。PA 的工作是配置必要的 PEP 以启用连接。根据 ZTA 的部署方式，这可能涉及向网关和代理或资源门户发送身份验证结果和连接配置信息。PA 还负责根据策略终止连接（例如，超时后，工作流完成时，或由于安全警报）。

2.1）信任算法的变体

实现 ZTA 信任算法（TA，Trust Algorithm）的方法有很多种。不同的实现者可能希望根据其感知到的重要性，对上述因素进行不同的权衡。还有两个主要特征可以用来区分 TA。第一个是如何评估这些因素，要么是二元决策，要么是整个“分数”的加权部分；第二个是如何评估与同一用户（或应用程序）ID 的其他请求有关联的那些请求。

•基于准则与基于分数：基于准则的 TA，假设在授予资源访问权限之前必须满足一组合格属性。这些条件由企业配置，应为每个资源独立配置。只有在满足所有条件时，才授予对资源的访问权限。基于分数的 TA，基于每个数据源的值和企业配置的权重，计算“分数”。如果分数大于资源的配置阈值，则授予访问权限。否则，访问被拒绝。

•单一（Singular）与上下文（Contextual）：单一 TA 会单独处理每个请求，在进行评估时不考虑用户/应用程序的历史情况。这样可以加快评估速度，但如果一种攻击驻留在用户被允许的角色内，则存在风险无法检测到这个攻击。上下文 TA 在评估访问请求时会考虑用户（或网络代理）的最近历史记录。这意味着 PE 必须维护所有用户和应用程序的某些状态信息，但更有可能检测到攻击者使用被攻陷的凭证以访问信息，其模式与 PE 为给定用户/代理看到的有所不同。

这两种因素并不相互依赖。可能有一个 TA，它将信任分数分配给每个用户和/或设备，并且仍然独立地考虑每个访问请求（即单一的）。同样，另一个不同的 TA 可以是基于分数的，但同时也是上下文的，即每个成功和失败的访问请求都可以用来更改最终信

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

任分数值。

理想情况下，ZTA 信任算法应该是上下文的，但这并不总是可能的。它可以缓解这种威胁：当攻击者非常接近一组“正常”的针对一个失陷用户账户（或内部攻击）的访问请求。在定义和实现信任算法时，必须平衡安全性、可用性和成本效益。依据用户在组织中的任务功能和角色的历史趋势和规范，不断地提示用户，要针对其行为进行重新认证，可能会导致可用性问题。例如，如果一个机构的人力资源部门的员工通常在一个典型的工作日内访问 20-30 个员工记录，则上下文 TA 可能会在访问请求一天内突然超过 100 个记录时发送警告，因为这可能是攻击者使用失陷的人力资源账户外渗记录。这是一个上下文 TA 可以检测到攻击，而单个 TA 可能无法检测到新行为的例子。另一个例子是一个会计，他通常在正常工作时间访问财务系统，而现在正试图在半夜从一个无法识别的位置，访问该系统。上下文 TA 可能触发警告，并要求用户满足 NIST SP 800-63A 中规定的更严格分数或其他准则。

为每个资源开发一组准则或权重/阈值，需要规划和测试。在 ZTA 的初始部署过程中，企业管理员可能会遇到这样的问题：由于配置错误导致本应该批准的访问请求遭到拒绝。这将导致部署的初始“优化”阶段。可能需要调整准则或评分权重，以确保在执行策略的同时仍允许企业的业务流程正常工作。

3）网络组件

在 ZTA 网络中，用于控制和配置网络的通信流，与用于执行组织的实际工作的应用程序通信流之间，应该存在隔离（逻辑的或可能是物理的）。这通常被分解为用于网络控制通信的控制平面和用于应用通信流的数据平面[Gilman]。

控制平面被各种基础设施组件用于维护系统；判断、授予或拒绝对资源的访问；以及执行任何必要的操作以建立资源之间的连接。数据平面用于应用程序之间的实际通信。在通过控制平面建立连接之前，该通信信道可能是不可能的。例如，PA 和 PEP 可以使用控制平面在用户和企业资源之间建立连接。然后，应用程序工作负载才能使用已建立的数据平面连接。

3.1）支持 ZTA 的网络需求

企业系统应具有基本的网络连接性。本地网络提供基本的路由和基础设施（如 DNS 等）。远程企业系统不一定使用所有基础设施服务。

1.企业必须能够确定哪些系统是企业拥有或管理的，哪些设备不是企业拥有或管理的。这取决于企业发放的凭据，而非未经验证的信息（例如，MAC 地址等）。

2.企业能够捕获所有网络流量。企业能够记录在数据平面上看到的数据包，但可能无法对所有数据包执行深度数据包检查（DPI）。企业能够过滤出关于连接的元数据（例如，目的地、时间、设备标识等）。

© 2020 奇安信集团 保留所有权利

奇安信身份安全实验室出品

3. 未访问 PEP 时，不应该发现企业资源。企业资源不接受来自 Internet 的任意传入连接。资源仅在客户端经过身份验证后，接受自定义配置的连接。这些连接是由 PEP 建立的。这可防止攻击者扫描网络以识别目标并对资源发起 DoS 攻击。

4. 数据平面和控制平面在逻辑上是分开的。PE、PA 和 PEP 都是在逻辑上独立、企业系统和资源无法访问的网络上进行通信。企业系统在执行网络任务时使用数据平面。PE、PA 和 PEP 使用控制平面来通信和管理系统之间的连接。PEP 必须能够发送和接收来自数据平面和控制平面的信息。

5. 企业系统可以到达 PEP 组件。企业用户必须能够访问其企业 ZTA 网络上的 PEP 组件，以访问资源。可以采用的方式有企业系统上启用连接的 Web 门户或软件代理。

6. PEP 是唯一可以访问 PA 和 PE 的组件。在企业网络上运行的每个 PEP 都有一个与 PA 的连接，以便从客户端建立连接。PA 可以被发现，但只有 PEP 才允许连接。

7. 远程企业系统应能够访问企业资源，而无需穿越企业基础设施。例如，不应要求远程用户使用回连到企业网络的安全链接（即 VPN）来访问由企业使用并由公共云提供商托管的服务（例如电子邮件）。

8. 企业系统由于可观察因素而可能无法达到某些 PEP。

例如，移动系统可能无法到达某些资源，除非它们使用企业网络基础设施。这些因素可能基于位置（地理位置或网络位置）、设备类型等。

六、部署场景/用例

任何企业网络都可以在设计时考虑零信任原则。如今，大多数组织的企业基础架构已经具有了零信任的某些要素，或者正在通过实施信息安全和弹性策略以及最佳实践来实现。有几种场景可以更轻松地实施零信任体系架构。例如，ZTA 易于在地理广泛分布和/或具有高度移动性的员工队伍的组织中扎根。也就是说，任何具有多种资源的大型网络的组织，都可以从零信任架构中获益。

在下面的用例中，没有明确指出 ZTA，因为企业可能同时拥有遗留和（可能）ZTA 基础设施。ZTA 组件和遗留网络基础设施在企业中同时运行可能会有一段时间。

1）拥有多分支机构的企业

最常见的情况是，企业只有一个总部和一个或多个地理上分散的位置，这些位置没有企业拥有的物理网络连接（见图 8）。远程位置的员工可能没有完全由企业拥有的本地网络，但仍需要访问企业资源才能执行其任务。同样，员工也可以使用企业拥有或个人拥有的设备，进行远程工作或在远程位置工作。在这种情况下，企业可能希望授予对某些资源（如员工日历、电子邮件）的访问权限，但拒绝访问更敏感的资源（如人力资源

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

数据库）。

在这个用例中，PE/PA 最好作为一个云服务托管，终端系统有一个连接代理（见第 3.1.1 节）或访问一个资源门户（见第 3.1.3 节）。由于远程办公室和工作人员必须将所有流量发送回企业网络才能访问云服务，因此将 PE/PA 托管在企业本地网络上可能不是响应最迅速的。

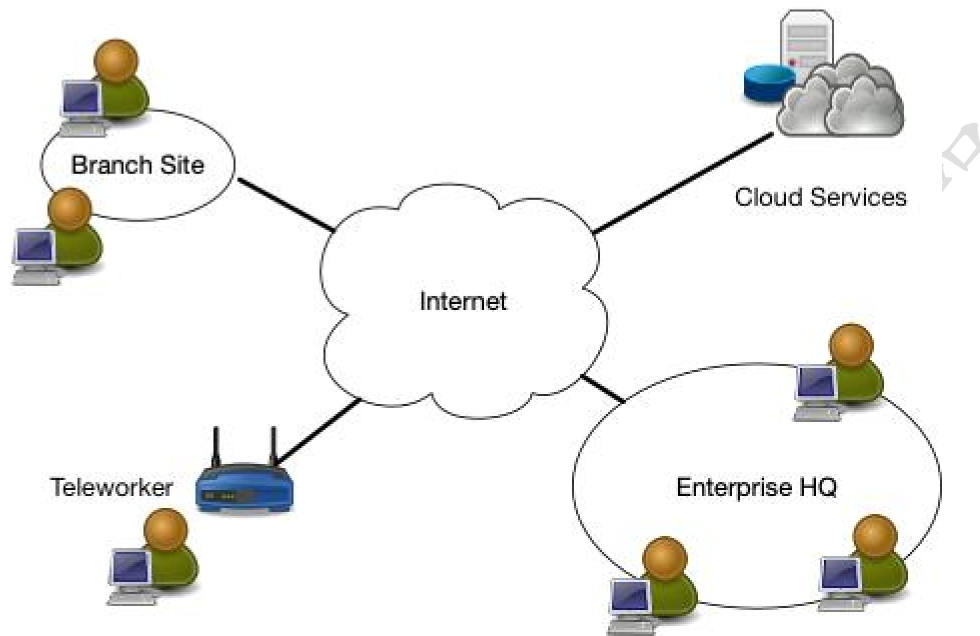


图 8：拥有远程员工的企业

2）多云企业

部署 ZTA 策略的一个越来越常见的用例是使用多个云提供商的企业（见图 9）。在这个用例中，企业有一个本地网络，但使用两个（或更多）云服务提供商来承载应用程序和数据。有时，应用程序，而非数据源，托管在一个独立的云服务上。为了提高性能和便于管理，托管在云提供商 A 中的应用程序，应该能够直接连接到托管在云提供商 B 中的数据源，而不是强制应用程序通过隧道返回企业网络。

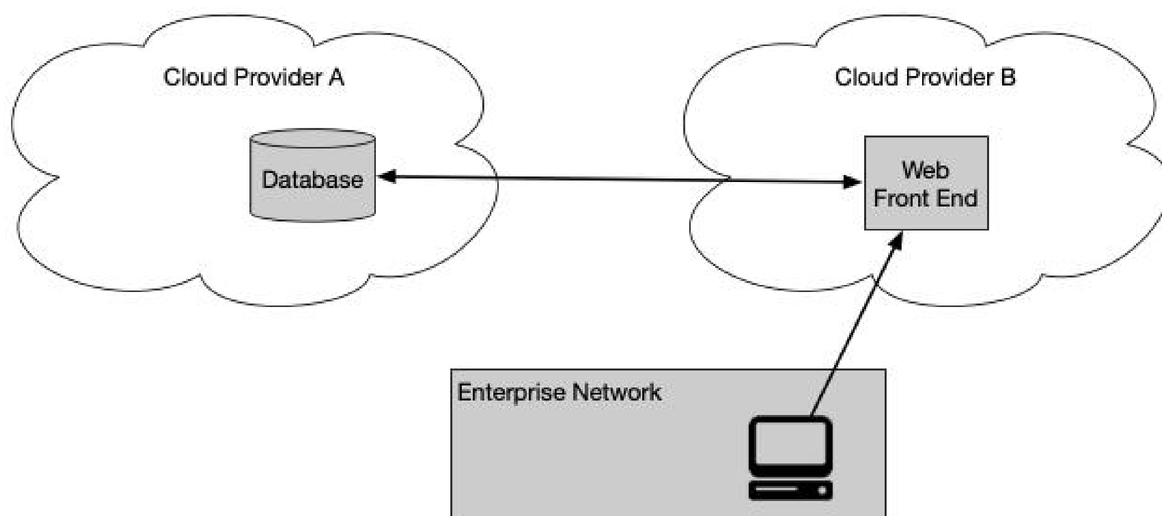


图 9：多云用例

这个多云用例是 ZTA 采用的主要驱动因素之一。它是 CSA 的 SDP 规范的服务器到服务器实现。随着企业转向更多的云托管应用程序和服务，依赖企业边界进行安全保护显然成为一种负担。如第 2.2 节所述，ZTA 认为，企业拥有和运营的网络基础设施与任何其他服务提供商拥有的基础设施之间应该没有区别。多云使用的零信任方法，是在每个应用程序和数据源的访问点放置 PEP。PE 和 PA 可以是位于云或甚至第三个云提供商上的服务。然后，客户端（通过门户或本地安装的代理）直接访问 PEPs。这样，即使托管在企业外部，企业仍然可以管理对资源的访问。

3）存在外包服务和/或非员工访问的企业

另一个常见的场景是，一个企业包含需要有限访问企业资源才能完成工作的现场访问者和/或外包服务提供商（见图 10）。例如，企业有自己的内部应用程序、数据库和员工工作系统。这些包括外包给偶尔在现场提供维护任务的供应商的服务（例如，由外部供应商拥有和管理的智能暖通空调（HVAC）系统和照明系统）。这些访客和服务提供商将需要网络连接来执行他们的任务。ZTA 网络可以通过允许这些设备（以及任何来访的服务技术人员）访问 Internet 来实现这一点，同时还可以屏蔽企业资源。

© 2020 奇安信集团 保留所有权利

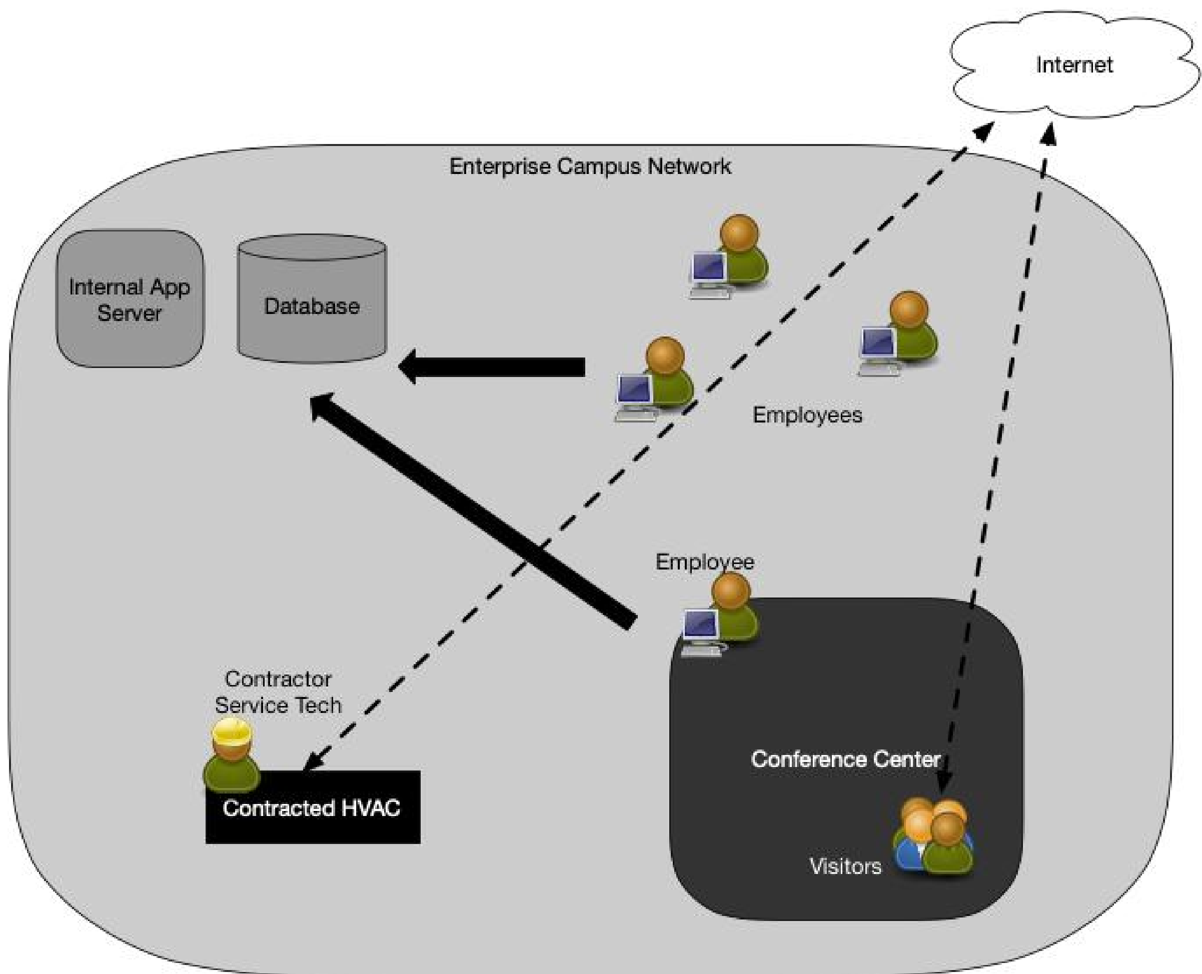


图 10：具有非员工访问的企业

在本例中，该组织还有一个会议中心，访客可以在其中与员工进行交互。同样，通过 ZTA 的 SDP 策略，员工设备和用户是有区别的，可以分别访问恰当的企业资源。进入校园的访客可以访问 Internet，但不能访问企业资源。它们甚至不能进行网络扫描，以查找可能可见的企业服务（即阻止主动网络侦察）。

在这个用例中，PE 和 PA 可以作为云服务或在 LAN 上托管（假设很少或根本没有使用云托管服务）。企业系统可以安装代理或通过门户访问资源。PA 确保所有非企业系统（那些没有安装代理或无法连接到门户的系统）不能访问本地资源，但可以访问 Internet。

4）跨企业协同

第四个用例是跨企业协作。例如，有一个项目涉及企业 A 和企业 B 的员工（见图 11）。这两个企业可以是独立的联邦机构（G2G），甚至是联邦机构和私营企业（G2B）。企业 A 运行用于项目的数据库，但必须允许企业 B 的某些成员访问数据。企业 A 可以为企业 B 的员工设置专用账户，以访问所需的数据并拒绝访问所有其他资源。

© 2020 奇安信集团 保留所有权利

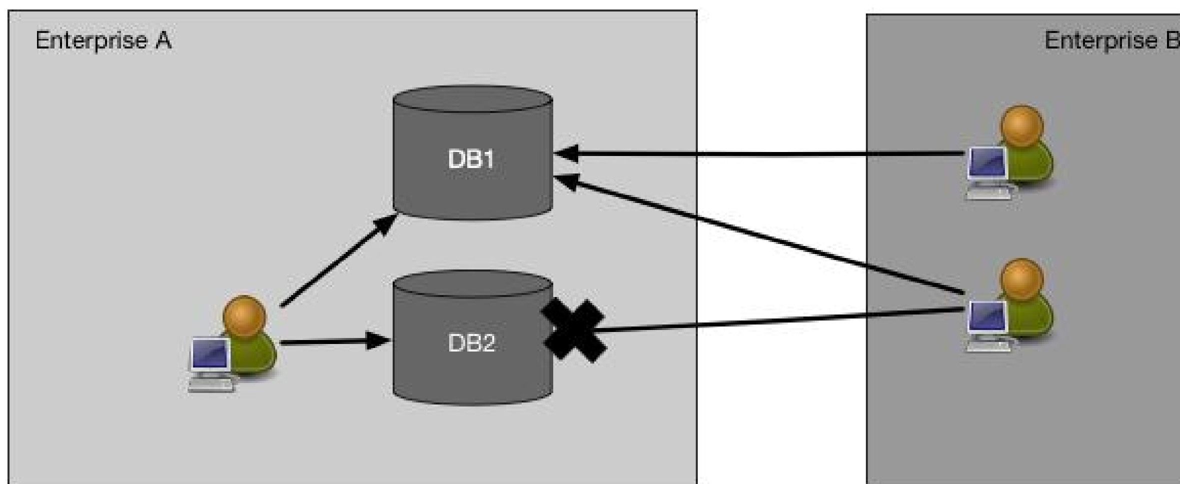


图 11：跨企业协作

此场景可以类似于上面的用例 1，因为两个企业的员工可能不在其组织的网络基础设施上，并且他们需要访问的资源可能在一个企业网络内部或托管在云中。这意味着不需要复杂的防火墙规则或企业范围的 ACL，允许属于企业 B 的某些 IP 地址访问企业 A 中的资源。如何完成此访问，取决于使用的技术。与用例 1 类似，PE 和 PA 在理想情况下将作为云服务托管。企业 B 的员工可能会被要求在其系统上安装软件代理或通过 Web 代理网关访问必要的数据资源。

七、与零信任架构相关的威胁

任何企业都不能完全消除网络安全风险。当与现有的网络安全政策和指南、身份和访问管理、持续监测、一般的网络卫生共用时，ZTA 可以减少整体风险暴露和保护共同威胁。不过，ZTA 也存在一些独特的威胁风险。

1）ZTA 决策过程的受损

在 ZTA 中，PE 和 PA 组件是整个企业的关键组件。企业资源之间不会发生连接，除非经过 PE 和 PA 批准和可能的配置。这意味着必须正确配置和维护这些组件。任何具有 PE 规则的配置访问权限的企业管理员，都可以执行未经批准的更改（或误操作），这些更改可能会中断企业运行。同样，失陷的 PA 可能允许访问未经批准的资源（例如，受损的个人拥有设备）。

要缓解相关风险，必须正确配置和监控 PE 和 PA 组件，并且必须记录任何配置更改并接受审计。

© 2020 奇安信集团 保留所有权利

2）拒绝服务或网络中断

在 ZTA 中，PA 是资源访问的关键组件。未经 PA 的许可和可能的配置操作，企业资源不能相互连接。如果攻击者中断或拒绝对 PEP 或 PA 的访问（即拒绝服务攻击），则可能对企业操作造成不利影响。

大多数企业可通过将策略强制驻留在云中或按照网络弹性指南在多个位置备份，来缓解此威胁。

3）内部威胁

正确实施 ZTA 策略、信息安全和弹性策略、最佳实践，可以降低内部攻击的风险。ZTA 确实可以防止失陷的账户或系统,访问其正常权限之外或正常访问模式之外的资源。为网络访问实施 MFA 还可以降低从失陷账户访问的风险。但是，与传统企业一样，具有有效凭证的攻击者（或恶意内部人员）可能仍然能够访问已授予账户访问权限的资源。

ZTA 增强了对该攻击的抵抗力，并防止任何失陷的账户或系统在整个网络中横向移动。此外，上下文 TA 比传统网络更容易检测到此类攻击并快速响应。上下文 TA 可以检测出超出正常行为的访问模式，并拒绝失陷账户（或内部威胁）访问敏感资源。

4）网络可见性

ZTA 需要检查并记录网络上的所有流量，并对其进行分析，以识别和应对针对企业的潜在攻击。然而，如前所述，企业网络上的一些（可能是大多数）流量对于网络分析工具来说可能是不透明的。此流量可能来自非企业所有的系统（例如，使用企业基础设施访问 Internet 的外包服务）或抗被动监视的应用程序。企业无法执行 DPI 或检查加密的通信，必须使用其他方法评估网络上可能的攻击者。

这并不意味着企业无法分析它在网络上看到的加密流量。企业可以收集有关加密流量的元数据，并使用这些元数据检测网络上可能存在的恶意软件通信或活动攻击者。机器学习技术可用于分析无法解密和检查的流量。采用这种类型的机器学习，将允许企业将流量分类为有效的，或可能恶意并需要补救的。在 ZTA 部署中，只需要检查来自非企业所有系统的流量，因为所有企业流量都经过了 PA（通过 PEP）的分析。

5）网络信息的存储

网络流量分析的一个相关威胁是分析组件本身。如果存储网络流量和元数据以进行进一步分析，则该数据将成为攻击者的目标。与网络拓扑、配置文件和其他各种网络架构文档一样，这些资源也应该受到保护。如果攻击者能够成功地访问存储的流量信息，则他们可能能够深入了解网络架构并识别资产以进行进一步的侦察和攻击。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

ZT 网络上攻击者的另一个侦察信息来源是用于编码访问策略的管理工具。与存储的通信流量一样，此组件包含对资源的访问策略，可以向攻击者提供最有价值的账户信息（例如，可以访问所需数据资源的账户）。

与所有有价值的企业数据一样，应提供足够的保护，以防止未经授权的访问和访问尝试。由于这些资源对安全至关重要，因此它们应该具有最严格的访问策略，并且只能从指定（或专用）管理员账户进行访问。

6）对专有数据格式的依赖

ZTA 依赖多个不同的数据源来做出访问决策，包括关于请求用户的信息、使用的系统、企业和外部情报、威胁分析等。通常，用于存储和处理这些信息的系统在如何交互和交换信息方面没有一个通用的、开放的标准。与 DoS 攻击一样，这种风险并非 ZTA 独有，但由于 ZTA 严重依赖信息的动态访问（企业和服务提供商双方），中断可能会影响企业的核心业务功能。

为降低相关风险，企业应综合考虑供应商安全控制、企业转换成本、供应链风险管理等因素，对服务提供商进行评估。

7）ZTA 管理中非个人实体（NPE）的使用

人工智能（AI）和其他基于软件的代理正在部署，以管理企业网络上的安全问题。这些组件需要与 ZTA 的管理组件（例如，PE、PA 等）交互，有时代替了人工管理员。在实施 ZTA 策略的企业中，这些组件如何对自己进行身份验证是一个开放性问题。假设大多数自动化技术系统在使用到资源组件的一个 API 时，将使用某种方式进行身份验证。

相关的风险是，攻击者将能够诱导或强制 NPE 代理执行某些攻击者无权执行的任务。与人类用户相比，软件代理可能具有较低的认证标准（例如，API 密钥与 MFA），以执行管理或安全相关任务。还有一个潜在的风险是，攻击者可以在执行任务时访问到软件代理的凭证并模拟该代理。

八、零信任架构与现有联邦指南

有一些现有的联邦政策和指南，与 ZTA 战略的规划、部署和运行相交叉。当与现有的网络安全政策和指南、身份凭证和访问管理（ICAM）、持续监测、通用的网络卫生结合时，ZTA 可以加强组织的安全姿态并防护共同威胁。

笔者说明：由于此节内容所涉及到的美国各种政策指南，具有美国政府的特定性，且与理解零信任关系不大，故只摘录简要内容。

奇安信身份安全实验室出品

1）ZTA 和 NIST 风险管理框架

ZTA 部署涉及围绕指定任务或业务流程的可接受风险，制定访问策略。必须识别、评估和缓解与执行给定任务相关的风险。为此，NIST 制定了风险管理框架（RMF）。

ZTA 的规划和实施可能会改变企业定义的授权边界。这是由于添加了新组件（例如，PE、PA 和 PEP）以及减少了对网络外围防御的依赖。RMF 中描述的过程不会改变 ZTA 的网络安全策略。

2）ZTA 和 NIST 隐私框架

隐私和数据保护包括在 FISMA 和 HIPAA 等合规计划中。而 ZTA 的核心要求之一是，企业应检查并记录其网络上的所有流量。这包括尽可能对通信量进行解密以启用检查。某些流量可能包含私人信息或具有相关的隐私风险。NIST 隐私框架有助于开发一个正式的流程，以识别和缓解 ZTA 网络的任何隐私相关风险。

3）ZTA 和联邦身份、凭证和访问管理架构（FICAM）

用户配置是 ZTA 的关键组成部分。如果 PE 没有足够的信息来标识关联的用户和资源，则 PE 无法决策尝试的连接是否应被授权连接到资源。在迁移到更为零信任的部署之前，需要制定强大的用户配置和身份验证策略。企业需要有一组清晰的用户属性和策略，PE 可以使用这些属性和策略来评估访问请求。

由于 ZTA 严重依赖于精确的身份管理，任何 ZTA 的努力都需要与机构的 ICAM 政策相结合。

4）ZTA 和可信 Internet 连接（TIC）

TIC 是由 OMB、DHS 和总务管理局（GSA）联合管理的一项联邦网络安全计划，旨在建立整个联邦政府的网络安全基线。

TIC 3.0 专注于基于网络的安全保护，而 ZTA 则是一个更具包容性的架构，用于解决应用程序、用户和数据保护问题。随着 TIC 3.0 用例的发展，很可能会开发一个 ZTA TIC 用例，来定义将在 ZTA 强制实施点部署的网络保护。

5）ZTA 和 EINSTEIN（NCPS-国家网络安全保护系统）

NCPS（又名 EINSTEN（爱因斯坦））是一个集成的体系，提供入侵检测、高级分析、信息共享和入侵防御能力，以保护联邦政府免受网络威胁。NCPS 的目标与零信任的首要目标一致，是管理网络风险，改进网络保护，并授权合作伙伴保护网络空间。

奇安信身份安全实验室出品

NCPS 传感器的部署基于联邦政府的周界网络防御，而零信任架构使保护更接近数据和资源。如果整个联邦政府都采用 ZTA，则 NCPS 的实施需要改进，或者需要部署新的能力来实现 NCPS 目标。

6）ZTA 和持续诊断和缓解（CDM）计划

国土安全部 CDM 计划是一项旨在改善联邦机构 IT 安全状况的努力。这种态势的关键是，机构要洞察机构内的系统、配置和用户。

有一个强大的 CDM 计划是 ZTA 成功的关键。国土安全部 CDM 计划已经启动了几项工作，以建立联邦机构内所需的能力，从而转向 ZTA 战略。

7）ZTA、云智能和联邦数据战略

云智能战略、更新的数据中心优化计划政策、联邦数据战略等政策，要求机构清点和评估它们如何收集、存储和访问本地和云中的数据。

该清单对于确定哪些业务流程和资源将从实施 ZTA 中受益至关重要。主要基于云或主要由远程工作者使用的数据资源和应用程序，是 ZTA 方法的良好候选，因为用户和资源都位于企业网络周界之外。

九、迁移到零信任架构

实施 ZTA 战略是一个旅程，而非对基础设施或流程的大规模替换。组织应该逐步实现零信任原则、流程变更、保护其最高价值数据资产的技术解决方案。

企业如何迁移到 ZTA 战略，取决于其当前的网络安全态势和运行情况。企业应该达到一个能力基线，包括为企业识别和编目资产、用户和业务流程。企业在开发一系列 ZTA 候选业务流程和参与此流程的用户/系统之前，需要此信息。

1）纯零信任架构

可以从头开始构建一个零信任架构网络。假设企业知道所需使用的应用程序和工作流，那么它可以为这些工作流生成基于零信任策略原则的架构。一旦确定了工作流，企业就可以缩小所需组件的范围，并开始映射各个组件的交互方式。从这一点上讲，它是一个构建网络基础设施和配置组件的工程实践。

当然，组织的网络通常不会是新建的。然而，有时一个组织可能会被要求履行一项新的职责，这将需要建立它自己的网络基础设施。在这种情况下，有可能在某种程度上引入 ZT 概念。例如，一个机构可能被赋予一项新的职责，即建立一个新的应用程序和数据库。该机构可以围绕 ZT 原则，设计新需要的基础设施，例如在授予访问权限之前

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

评估用户的信任，在新资源周围部署微周界等。

2）混合 ZTA 和传统架构

ZTA 工作流与传统企业架构的共存，可能会有一段时间。企业向 ZTA 方法的迁移，可以采取一次迁移一个业务流程的方式。企业需要确保公共元素（例如 ID 管理、设备管理、事件日志等）足够灵活，以在 ZTA 和遗留混合安全架构中运行。企业架构师也可能希望将 ZTA 候选解决方案，限制为那些可以与现有组件接口连接的解决方案。

3）将 ZTA 引入传统架构网络的步骤

笔者说明：此小节内容是本篇中的关键，详述了在传统架构网络中采取渐进方式逐步引入零信任架构的**“七步走”**部署策略。

迁移到 ZTA，需要组织对其资产（物理和虚拟）、用户、业务流程有详细的了解。当评估资源请求时，PE 可以访问这些知识。不完整的知识，通常会导致业务流程失败，即 PE 由于信息不足而拒绝请求。

在努力把 ZTA 带到企业之前，应该对资产和用户进行调查。这是在 ZTA 部署之前应该达到的基础状态。这些调查可以并行进行，但都与对组织业务流程的检查有关。这些步骤可以映射到风险管理框架（RMF）中的步骤，因为向 ZTA 的任何转移，都可以看作是降低机构业务职能风险的过程。通往 ZTA 的路径如图 12 所示。

奇安信身份安全实验室出品

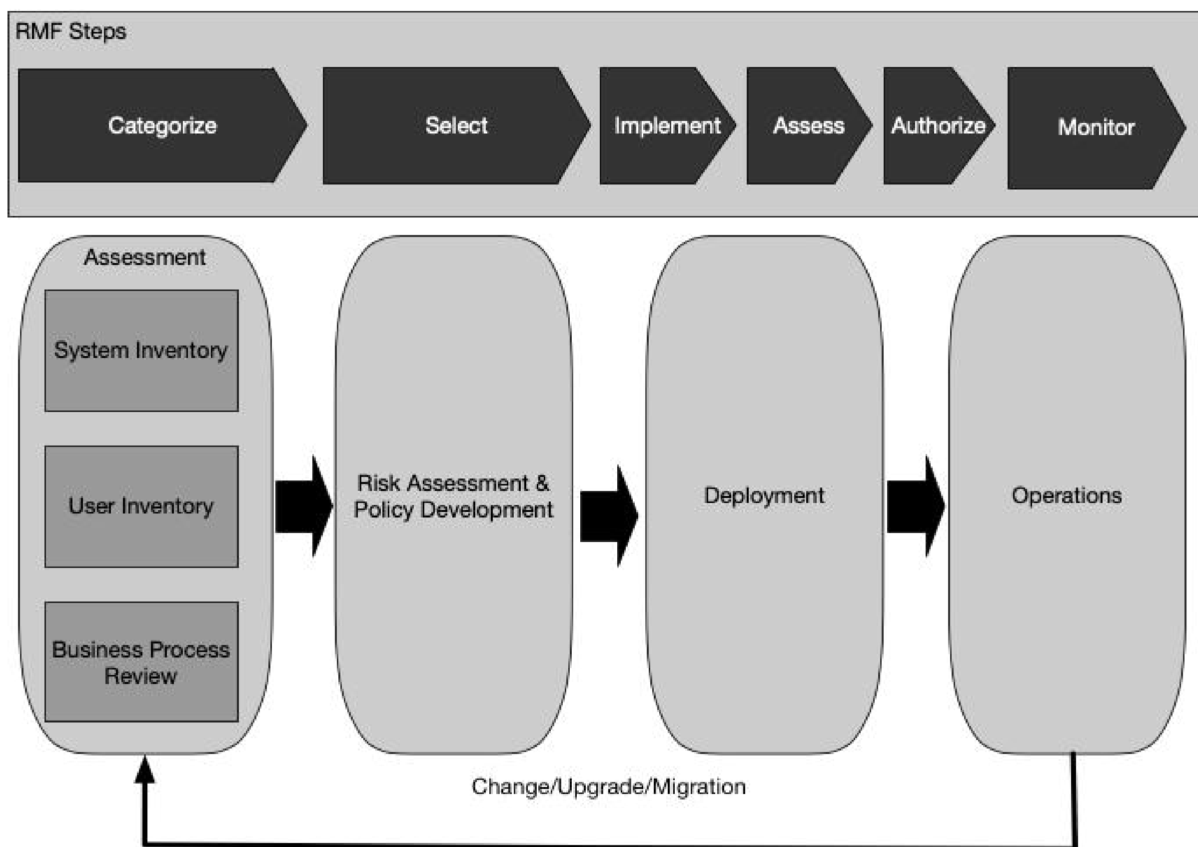


图 12:ZTA 部署周期

创建初始库存清单后，将会有定期的维护和更新周期。此更新可能会更改业务流程或不产生任何影响，但应进行业务流程评估。例如，数字证书提供商中的变更，可能看起来没有重大影响，但可能涉及证书根存储管理、证书透明日志监视和其他起初不大明显的因素。

3.1）识别企业中的参与者

为了 ZTA 网络的运行，PE 必须具备企业主体的知识。“主体”包括人和可能的非人实体（NPE），例如与资源交互的服务账户。

具有特殊权限的用户（如开发人员或系统管理员），在被分配属性或角色时需要特别考虑。在传统的安全架构中，这些账户可能具有访问所有企业资源的总体权限。ZTA 应该允许开发人员和管理员有足够的灵活性，来满足他们的业务需求，但同时要记录和审核行为。

3.2）识别企业拥有的资产

ZTA 的关键要求之一是识别和管理企业自有设备的能力。ZTA 还要求能够识别和监

© 2020 奇安信集团 保留所有权利

控可能在企业拥有的网络基础设施上或访问企业资源的非企业拥有的设备。管理企业资产的能力是 ZTA 成功部署的关键。这包括硬件组件（例如笔记本电脑、电话、物联网设备等）和数字化构件（例如用户账户、应用程序、数字证书等）。

这不仅仅是对企业资产数据库进行编目和维护。这还包括配置管理和监视。观察系统当前状态的能力，是评估访问请求过程的一部分。这意味着企业必须能够配置、调查和更新企业系统，包括虚拟系统、容器等。这还包括其物理位置（最佳估计）和网络位置。此信息应在做出资源访问决策时通知给 PE。

非企业所有的资产也应尽可能地分类。这可能包括企业可见的任何内容（例如，MAC 地址、网络位置），并通过管理员数据输入进行扩充。这些信息不仅用于访问决策（因为合作者和 BOYD 系统可能需要联系 PEP），还用于企业的监控。

许多联邦机构已经开始了识别企业资产的任务。已经建立了 CDM 能力如硬件资产管理（HWAM）和软件资产管理（SWAM）的机构，在制定 ZTA 战略时有一套丰富的数据可供参考。各机构还可能有一份涉及高价值资产的 ZTA 候选流程清单，这些流程已被确定为机构任务的关键。

3.3）识别关键流程并评估与执行流程相关的风险

一个机构应该进行的第三项清查，是识别和排列该机构的业务流程（即任务）。业务流程应通知在何种情况下授予和拒绝资源访问请求。企业在第一次过渡到 ZTA 时可能希望从低风险的业务流程开始，因为中断可能不会对整个组织产生负面影响。一旦获得了足够的经验，就可以选择更关键的业务流程。

利用基于云的资源或由远程工作人员使用的业务流程，通常是 ZTA 的良好候选。这是因为客户端和资源不在企业范围内，这是 ZTA 相对于传统企业网络架构的主要优势之一。**企业客户端可以直接请求云服务，而不是通过虚拟专用网（VPN）将企业边界投射到云中或将客户端带入企业网络。**企业的 PEP 确保在将资源访问权授予客户机之前遵循企业策略。

3.4）为 ZTA 候选制定策略

识别候选应用程序或业务工作流的过程，取决于以下几个因素：流程对组织的重要性、受影响的用户组、工作流所用资源的当前状态。基于资产或工作流风险的资产或工作流的价值，可以使用 NIST 风险管理框架进行评估。

识别资产或工作流后，下一步是识别将受影响的用户集。这可能会影响作为第一次迁移到 ZTA 的候选者的选择。由企业用户的已识别子集（例如，采购系统）所使用的应用程序，可以优先于对企业的整个用户群至关重要的应用程序（例如，电子邮件）。

然后，企业管理员需要为候选业务流程中使用的资源，确定一组准则（如果使用基

© 2020 奇安信集团 保留所有权利

于准则的 TA）或信任分数权重（如果使用基于分数的 TA）。管理员可能需要在优化阶段对这些条件或值进行调整。这些调整是必要的，以确保策略有效，但又不妨碍对资源的必要访问。

3.5）确定候选解决方案

一旦开发了一系列候选业务流程，企业架构师就可以编写一系列候选解决方案。一些部署模型更适合于特定的工作流和当前的企业生态系统。而一些供应商解决方案比其他解决方案更适合于特定的用例。需要考虑的因素有：

- 解决方案是否要求在客户端系统上安装组件？这可能会对那些使用了非企业拥有系统（如 BYOD 或跨机构协作）的业务流程产生限制。
- 解决方案是否用于业务流程资源完全存在于企业内部的场景？一些解决方案假设请求的资源将驻留在云中（所谓的“南北”流量），而不是企业范围内（“东西”流量）。候选业务流程资源的位置，将影响到该流程的候选解决方案和 ZTA。

一种解决方案是将现有业务流程建模为试点计划，而不仅仅是替换。这个试点计划可以通用化，以应用于多个业务流程或特定于一个用例。

3.6）初始部署和监测

一旦选择了候选工作流和 ZTA 组件，就可以开始初始部署。企业管理员必须使用选定的组件来实现已开发的策略，但首先可能希望使它们更为宽松。很少有企业策略集在第一次迭代中就是完整的：重要的用户账户（例如，管理员账户）可能被拒绝访问他们需要的资源，也可能不需要他们分配的所有访问特权。

新的 ZT 业务工作流可以在“仅报告模式”下运行一段时间，以确保策略的有效性和可操作性。“仅报告”意味着应为大多数请求授予访问权限，并且应将连接的日志和踪迹与最初制定的策略进行比较。基本策略，如拒绝掉 MFA 失败的请求或出现在已知黑名单 IP 地址中的请求，都应该强制执行并记录，但是在初始部署之后，访问策略应该更宽松些，以收集 ZT 工作流实际交互的数据。如果无法以更宽松的方式运行，企业网络运行人员应密切监视日志，并准备根据运行经验修改访问策略。

3.7）扩展 ZTA

在工作流策略集获得足够的信任后，企业进入了稳定的运行阶段。在此阶段，企业管理员可以开始规划 ZT 部署的下一阶段。与上一次发布一样，需要确定候选工作流和解决方案集，并开发初始策略。

但是，如果工作流发生变更，则需要重新评估正在运行的 ZT 架构。对系统的重大变更，如新设备、软件（特别是 ZT 逻辑组件）的重大更新、组织结构的变化，都可能

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

导致工作流或策略的变更。例如，购买了新设备，但没有创建新的用户账户，因此需要更新设备资源清单。

附录 A：缩略语

（略）

附录 B：识别 ZTA 当前技术水平的差距

对于零信任组件和解决方案的当前成熟度，在本文档的背景研究期间进行了调查。以下是 ZTA 生态系统和需要进一步调查的区域中识别出的差距的总结。

B.1 技术调查

多个供应商受邀展示了他们关于零信任的产品和观点。本次调查的目的是找出那些阻碍机构现在迁移到 ZTA 基础设施或维护现有 ZTA 部署的遗漏部分。这些差距可分类为即时部署（即时或短期）、影响维护或运行的系统性差距（短期或中期）、知识缺失（未来研究领域）。表 B-1 总结了这些内容：

表 B-1：识别的差距汇总

分类	问题示例	识别的差距
立即性	如何编制采购要求 ZTA 战略如何与 TIC、FISMA 等结合。	缺乏 ZTA 的通用框架和词汇； 认识到 ZTA 与现行政策的冲突；
系统性	如何防止供应商锁定； 不同的 ZTA 环境如何相互作用；	过于依赖供应商 API；
研究领域	面对 ZTA，威胁将如何演变； 面对 ZTA，业务流程如何变化；	采用 ZTA 的企业中，成功的入侵是什么样的？ 采用 ZTA 的企业中的最终用户体验；

B.2 阻碍立即转移至 ZTA 的差距

这些都是目前阻碍 ZTA 战略采用的问题。这些问题被归类为“立即的”问题，并没有考虑今后的维护或迁移。

奇安信身份安全实验室出品

1）缺乏 ZTA 设计、规划和采购的通用术语

业界还没有一套术语或概念来描述 ZTA 的组件和运行。这使得组织（如联邦机构）很难为设计 ZTA 基础设施和采购组件制定一致的要求和政策。

2）关于 ZTA 与现有联邦网络安全政策冲突的认知

有一种误解，ZTA 是一个单一框架，带有一套解决方案，且与现有的网络安全观并不兼容。而实际上，零信任应该被视为当前网络安全战略的**演变**，因为许多概念和想法已经流传了很长时间。联邦机构已经被鼓励，通过现有的指南，采取更加零信任的方法，来解决网络安全问题。如果一个机构拥有成熟的 ID 管理系统和强大的 CDM 能力，那么它已经在通往 ZTA 战略的路上。这一差距其实是源于对 ZTA 的误解以及它是如何从以前的网络安全范式演变而来的。

B.3 影响 ZTA 的系统性差距

这些差距影响了 ZTA 战略的实施和部署，以及持续运营/成熟度。系统的差距是开放标准（由标准开发组织（SDO）或行业联盟制定）可以发挥助力的领域。

1）组件间接口的标准化

组件内部的互操作性问题，不仅发生在采购的时候，而且会随着时间推移。在更广泛的**零信任生态系统（ZTE）**中，组件的范围非常广泛，许多产品专注于 ZTE 内部的单个市场，并依赖于其他产品来向另一个组件提供数据或某些服务（例如，为资源访问而集成多因素认证（MFA））。

供应商常常依赖合作伙伴公司提供的专有 API，而不是标准化的、独立于供应商的 API 来实现这种集成。这种方法的问题在于，这些 API 是专有的，由单个供应商控制。一旦供应商改变 API 的行为，将导致集成商需要更新他们的产品来响应。这进一步增加了供应商和消费者的负担：供应商需要花费资源对其产品进行变更，当一个供应商对其专有 API 进行变更时，消费者需要对多个产品应用更新。

2）解决过度依赖专有 API 的新兴标准

目前，有多种模式和解决方案，试图建立 ZTA 的领导权威。这表明有机会开发一套开放的、标准化的协议（或框架），以帮助组织迁移到 ZTA 战略。标准开发组织（SDO）如 Internet 工程任务组（IETF）已经指定了在交换威胁信息时可能有用的协议。云安全联盟（CSA）已经为软件定义边界（SDP）开发了一个框架，该框架可能在 ZTA 中也很有用。

奇安信身份安全实验室出品

B.4 ZTA 的知识差距与未来研究方向

此节列出的差距，并不妨碍组织为其企业采用 ZTA 战略。这些是关于运行 ZTA 环境的知识的灰色区域。它们是未来研究人员的工作领域。

1）攻击者对 ZTA 的反击

对一个企业来说,一个正确实施的 ZTA 战略相对于传统的基于网络边界的安全而言,将改善其网络安全态势。ZTA 的宗旨是减少对攻击者的资源暴露，并在主机系统失陷时最小化（或防止）企业内部的横向移动。

然而，坚定的攻击者不会坐视不管，而是会改变面对 ZTA 的行为。开放性的问题是攻击将如何演变。一种可能性是，由于 ZTA 的主要原则之一是在访问资源之前进行频繁的身份验证，因此旨在窃取凭证的攻击（例如网络钓鱼、社会工程）可能会变得更加普遍。另一种可能性是，在混合型 ZTA/遗留企业中，攻击者将重点关注尚未应用 ZTA 原则的业务流程（即遵循传统的基于网络边界的安全）——实际上，目标是最容易摘到的果子，试图在 ZTA 业务流程中获得一些立足点。

随着 ZTA 的更加成熟，实现了更多的部署，并获得了经验，ZTA 相对于基于网络边界安全的旧方法的有效性将会变得显而易见。此外，还需要制定 ZTA 相对于较老网络安全策略的“成功”指标。

2）ZTA 环境中的用户体验

对于最终用户在使用 ZTA 战略的企业中表现得如何，还没有进行严格的审查。已有研究表明，用户对 MFA 和其他安全操作的反应，被视为 ZTA 企业战略的一部分。这项工作可以成为在企业中使用 ZTA 工作流时预测最终用户体验和行为的基础。

可以预测 ZTA 如何影响最终用户体验的一组研究，是 MFA 在企业中的使用和“安全疲劳”。安全疲劳是指最终用户面对如此多的安全策略和挑战，开始以负面方式影响其生产力的现象。一些用户很容易接受 MFA，如果这个过程是流畅的，并且涉及到他们习惯于使用或拥有的设备（例如，智能手机上的应用程序）。然而，有些用户讨厌在业务流程中使用个人拥有的设备，或者感到他们经常被监视以防对 IT 策略的可能触犯。

3）ZTA 对企业和网络中断的适应能力

对 ZTA 供应商生态系统的调查,显示了企业部署 ZTA 战略需要考虑的广泛基础设施。大多数被调查的产品和服务，都依赖于云的存在以提供健壮性，但众所周知即使是云服务也会在在遭遇攻击或简单错误时变得不可用。当这种情况发生时，用于做出访问决策的关键组件，可能无法访问或无法与其他组件通信。例如，位于云中的 PE 和 PA 组件，

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

可能在分布式拒绝服务(DDoS)攻击期间可访问,但可能无法访问所有位于资源中的PEP。需要研究如何发现ZTA部署模型的可能“瓶颈”以及ZTA组件不可访问或可访问性有限时对网络运行的影响。

在采用ZTA战略时，企业的运行连续性（COOP）计划可能需要修订。ZTA战略使许多COOP因素变得更容易，因为远程工作者可能与他们在本地拥有相同的资源访问权限。然而,如果用户没有得到适当培训而缺乏经验,像MFA这样的策略也可能产生负面影响。用户可能会在突发情况下忘记（或无法访问）令牌和企业设备，这将影响企业业务流程的速度和效率。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

NIST 标准《零信任架构》草案第 1、2 版全文对比与解读

编者按

2019 年 9 月 NIST 发布 Draft NIST Special Publication 800-207 后，开始广泛征求修改意见，并于 2020 年 2 月发布最新版本 Draft (2nd) NIST Special Publication 800-207。

在本文中，奇安信身份安全实验室将对两版标准进行了详细的对比。与 Draft1 相比，NIST 在 Draft2 中做了大量细致的修改及修正工作，并在原有基础上进行内容扩充新增部分章节。由此可见 NIST 对《零信任架构》标准的重视，正在加快标准推进的步伐。值得注意的是，Draft2 中对零信任历史的追溯到了国防信息系统局（DISA）和国防部（DOD）公布的“Black Core”（黑核）项目，将零信任标准与美国国防部建立了关联，可以推断出美国国防部也参与并影响了标准草案工作，一定意义上也是零信任标准加速的有力推手。

在详细对比 Draft2 与 Draft1 后，可以看出 NIST 认为更多的组织/机构能够受益于零信任架构。通过提供多种零信任实现方式，NIST 希望 ZTA 不仅能在大型企业落地，同时在小型企业中也能发挥作用。不管采用何种方式（增强的身份治理驱动、微分段、以及基于网络基础架构和 SDP 等）实现，ZTA 应该围绕着企业本身的资产防护且遵守零信任原则宗旨进行，而具体的实现方式应充分结合企业现状。同时，风险评估也成为零信任的重要内容之一，企业如果希望向 ZTA 迁移，在考虑技术替代的同时，也要重视风险评估工作。

NIST 在 Draft2 中再次强调**【零信任是一种以资源保护为核心的网络安全范式，其前提是信任从来不是隐式授予的，而是必须进行持续评估。】**Draft2 对 Draft1 的一些主要变化可以分为新增、修改两部分。

第一部分、新增部分

Draft2 中新增【3.1 零信任架构方法的变化】和【4.5 面向公众或客户提供服务的企业】两节。其中，3.1 节主要介绍了 ZTA 的三种实现方式：基于增强身份治理的 ZTA、采用微分隔的 ZTA、采用网络基础架构和 SDP 的 ZTA。在实践时，企业可以结合自身情

奇安信身份安全实验室出品

况采用一种或多种结合作为策略的主要驱动因素完成整体设计。4.5 节则是对部署场景/用例的补充。

另外，Draft2 中对【2.1 零信任的宗旨】进行了详细的修正，涉及多条修改，并新增一条原则（从 6 条增加到 7 条）：企业应尽可能收集有关网络基础架构和通信现状的信息，并利用这些信息改善安全姿态（security posture）。企业应该收集有关网络流量和访问请求的数据，然后使用这些数据来改进策略的创建和实施。此数据还可用于为来自主体的访问请求提供上下文。Draft2 针对 Draft1 中【3.3.1 支持 ZTA 的网络要求】，新增对于基础架构扩展性的要求（PE、PA 和 PEP 都是关键组成）；针对 Draft1 中【5.7 在 ZTA 管理中使用非人实体】，描述了误报的影响，提出可定期重新调整分析来纠正错误的决策并改进决策过程；针对 Draft1 中【7.3.2 识别企业拥有的资产】，新增加对影子资产的描述。总之，Draft2 中还新添多处细节内容，这里不再一一赘述，新增内容请参照下文详细对比部分。特别的，Draft2 新增 7 篇参考文献，为[BCORE]、[FIPS199]、[IBNVN]、[NISTIR 8062]、[NISTPRIV]、[SDNBOOK]、[SP800-63-3]。

第二部分、修改部分

Draft2 针对 Draft1 的主要修改包括读者群体、受益群体、ZT 和 ZTA 定义区分、保护对象、适用范围、向 ZTA 过渡前提等方面：

【读者群体】

读者群体由企业网络架构师修改为企业安全架构师。

【受益群体】

零信任/零信任架构的受益群体从 Draft1 中的“任何拥有具有多个资源的大型网络的组织”修改为“任何组织”。

【ZT 和 ZTA 定义区分】

Draft1 中未对 ZT 和 ZTA 明确定义，Draft2 中对 Draft1 对于 ZTA 的定义进修改，明确 ZT 和 ZTA 的定义。其中 ZT 主要指概念和思想，而 ZTA 则主要指利用 ZT 的企业网络安全规划，包括组件关系、工作流规划和访问策略。

【保护对象】

Draft2 删除了 Draft1 中“零信任是一种侧重于数据保护的体系架构方法”一条。在 Draft2 中修改为：安全防护应该围绕着“资产（数据、计算资产和应用等）”进行，不再只集中于对于数据的保护。

© 2020 奇安信集团 保留所有权利

【适用范围】

Draft2 对 Draft 2.1 零信任的宗旨修改补充：零信任的宗旨适用于在一个组织内部或与一个或多个合作伙伴组织协作完成的工作，不适用于面向公众或客户的业务流程。组织不能将内部的安全策略强加给外部参与者（例如，客户或普通互联网用户）。

【向 ZTA 过渡】

在 Draft1 中提出向“ZTA 过渡需要过程，需要全面的技术替换才可实现。”在 Draft2 中修改为“向 ZTA 过渡是关于组织如何评估其任务中的风险的过程，而不仅仅是简单地通过全面的技术替换就能实现。”除必要的技术替代外还需要重视风险评估。

在上文主要的修正之外，Draft2 也对标准中的措辞进行矫正，一些主要的矫正下表所示，更为细节请参照下文详细对比部分。

Draft1	Draft2	说明
Network（网络）	Enterprise environment（企业环境）	基本在整个标准中，用 enterprise environment（企业环境）替代了 network（网络）。将企业网络修正为企业环境更为准确。
Legacy mode（传统模式）	perimeter-based mode（基于边界的模式）	基本在整个标准中，用 perimeter-based mode（基于边界的模式）替代了 legacy mode（传统模式），明确指代基于边界的防护模式。
Connection（连接）	Communication path（通信路径）	基本在整个标准中，用 communication path（通信路径）替代了 connection（连接）。
Trust score（信任分）	Confidence level（信任度）	Draft2 更强调 confidence level（信任度），而不仅仅是 trust score（信任分），trust score（信任分）只是 confidence level（信任度）的一种代表方式。
Authentication（认证）	Authentication and authorization（认证和授权）	在 Draft2 中，对多处 authentication（身份认证）修正为 authentication and authorization（身份认证和授权），描述更为准确，对于权限除访问权限外还提到可以执行的操作（读/写）粒度。
/	Subject（主体）	对 Draft1 中，subject 定义为“用户/机器”，Draft2 修正 subject 为“用户、设备和应用的组合“。 在标准中相关的图中，都增加 subject（主体）。
/	Asset（资产）	在 Draft2 中明确定义，资产为“设备、基础架构和用户”。

Abstract 摘要

摘要中主要对前三句进行了修改。主要对零信任和零信任架构的定义进行修正和区分。在草案 2 中去掉了 strategy 的概念。

- 草案 1:【Zero Trust is the term for an evolving set of network security paradigms that move network defenses from wide network perimeters to narrowly focusing on individual or small groups of resources. A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). Access to data resources is granted when the resource is required, and authentication (both user and device) is performed before the connection is established.】

零信任（Zero Trust）是一种不断发展的网络安全范式的术语，这种范式将网络防御从广泛的网络边界转移到仅关注个体或一小部分资源。零信任体系结构（ZTA）战略是指不存在基于系统的物理或网络位置（即局域网与因特网）而授予系统隐式信任的战略。当需要资源时，授予对数据资源的访问权，并在建立连接之前执行身份认证（用户和设备）。

- 草案 2:【Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move network defenses from static, network-based perimeters to focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan enterprise infrastructure and workflows. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet). Authentication and authorization (both user and device) are discrete functions performed before a session to an enterprise resource is established.】

零信任（Zero trust，ZT）是一种不断发展的网络安全范式的术语，将网络防御从静态的、基于网络边界的防护转移到关注用户、资产和资源。零信任体系结构（ZTA）使用零信任原则来规划企业基础架构和工作流。零信任假定不存在仅仅基于物理或网络位置（即局域网与互联网）即授予资产或用户帐户的隐式信任。身份认证和授权（用户和设备）是在建立与企业资源的会话之前执行的独立功能。

Audience 读者群体

- 草案 1 中的【enterprise network architects】修改为草案 2 中的【enterprise security architects.】：即企业网络架构师，修改为企业安全架构师。
- 草案 1 中的【deploy ZTA concepts to an enterprise network.】修改为草案 2 中【deploy zero trust security concepts to an enterprise environment.】即：将 ZTA 概念部署到企业网络修改为将零信任安全概念部署到企业环境。
- 草案 1 中的【gain insight into ZTA from this document.】修改为草案 2 中的【gain insight into zero trust and ZTA from this document】即：将从本文档了解零信任架构修改为将从本文档了解零信任和零信任架构。

奇安信集团安全研究出品

Note to Reviewers

- 草案 1 中的【logical components of network infrastructure using a ZTA strategy.】修改为草案 2 中的【logical architectural components to develop and support a ZTA.】即：将"采用 ZTA 战略的网络架构的逻辑组件"修改为"开发和支持 ZTA 的逻辑架构组件"。

1. Introduction

- 草案 1 中 274 行，第一段最后增加一句：【Perimeter-based network security has also been shown to be insufficient since once attackers breach the perimeter, further lateral movement is unhindered.】即增加说明：【基于边界的网络安全也被证明是不够的，因为一旦攻击者突破边界，进一步的横向移动便会畅通无阻。】
- 草案 1 中 275 行，【a new way to plan enterprise network security known as Zero Trust Architecture (ZTA).】修改为【the development of a new model for cybersecurity principles and network security known as "zero trust" (ZT).】即：【一种新的企业网络安全规划方法称为零信任架构（ZTA)。】修改为【网络安全原则和网络安全新模式的发展称为"零信任"（ZT)。】
- 草案 1 中 276 行，【A ZTA approach】修改为【A ZT approach】。
- 草案 1 中 277 行，对企业资产进行了定义【all enterprise assets, such as devices, infrastructure, and users.】，企业的资产是包括设备、基础架构和用户。
- 草案 1 中 277 行，【ZTA assumes the network is hostile】修改为【Zero trust security models assume that an attacker is present on the network 】即：将【ZTA 假设网络是充满威胁的】修改为【零信任安全模型假设网络上存在攻击者】。
- 草案 1 中 278 行，【no more secure】修改为【no more trustworthy】即：【不再安全】修改为【不再值得信赖】。
- 草案 1 中 281 行，【In ZTA】修改为【In zero trust】。
- 草案 1 中 282 行，【minimizing access to resources to only those who are validated as needing access and continuously authenticating the identity and security posture of each access request.】修改为【minimizing access to

© 2020 奇安信集团 保留所有权利

resources (such as data and compute resources and applications) to only those users and asset identified as needing access as well as continually authenticating and authorizing the identity and security posture of each access request.”即【尽可能减少对资源的访问，只允许那些经过证实需要访问的人访问，并对每个访问请求的身份和安全姿态进行持续认证。】修改为【尽可能减少对资源（如数据、计算资源和应用）的访问，只允许那些被确定为需要访问的用户和资产访问，并对每个访问请求的身份和安全姿态进行持续认证和授权。】这其中对资源的范围进行了说明，资源包括数据、计算资源和应用，另外强调不止需要 authenticating 还需要 authorizing。

- 草案 1 中 284 行,开头增加一句【A zero trust architecture (ZTA) is an enterprise cybersecurity strategy that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement.】即:【零信任架构（ZTA）是一种基于零信任原则的企业网络安全战略，旨在防止数据泄露和限制内部横向移动。】这里对 ZT 和 ZTA 的关系进行了说明。
- 草案 1 中 286 行，【migrate to a ZTA-centered network infrastructure】修改为【migrate to a zero trust design approach to network infrastructure】即:【迁移到以 ZTA 为中心的网络基础架构】修改为【迁移到网络基础架构的零信任设计方法】。
- 草案 1 中 288 行，【ZTA】更正为【ZT】。
- 草案 1 中 288 行，【network infrastructure design】修改为【network infrastructure and system design】。
- 草案 1 中 290 行，明确参考了[FIPS199]。
- 草案 1 中 290 行,【Transitioning to ZTA is a journey and cannot be accomplished without a wholesale replacement of technology.】修改为【Transitioning to ZTA is a journey concerning how an organization evaluates risk in its mission and cannot simply be accomplished with a wholesale replacement of technology.】即:【向 ZTA 过渡是一个过程，如果没有全面的技术替换，就无法实现】修改为【向 ZTA 过渡是关于组织如何评估其任务中的风险的过程，而不仅仅是简单地通过全面的技术替换就能实现。】即强调 ZTA 的实现不是一蹴而就的，这个

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

过渡过程不是说堆砌一堆新技术去替代原来用技术就能成功实践，还需要关注组织自身进行风险评估的方式。

- 草案 1 中 293 行，【technology solutions that protect its data assets and business functions.】修改为【technology solutions that protect their data assets and business functions by use case.】即【保护其数据资产和业务功能的技术解决方案】修改为【通过用例保护其数据资产和业务功能的技术解决方案】。
- 草案 1 中 295 行，【hybrid Zero Trust/Legacy mode】修改为【hybrid zero trust/perimeter-based mode】即：【零信任/传统模式的混合模式】修改为【零信任/基于边界模式的混合模式】。
- 草案 1 中 297 行，【effective information security】修改为【comprehensive information security】，即：【有效的信息安全】修改为【全面的信息安全】。
- 草案 1 中 298 行，【complemented with existing cybersecurity policies】修改为【balanced with existing cybersecurity policies】即：【与现有的网络安全测略互补】修改为【与现有的网络安全策略相平衡】。
- 草案 1 中 299 行，【general cybersecurity】修改为【best practices】，即【一般的网络安全】修改为【最佳实践】。

1.1 History of Zero Trust Efforts Related to Federal Agencies

- 草案 1 中 302 行，1.1 节名从“背景”调整为“与联邦机构有关的零信任发展历史”。
- 草案 1 中 304 行，增加一句【The Defense Information Systems Agency (DISA) and the Department of Defense published their work on a more secure enterprise strategy dubbed “black core” [BCORE]. Black core involved moving from a perimeter-based security model to one that focused on the security of individual transactions.】即增加【国防信息系统局（DISA）和国防部（DOD）公布了他们在更安全的企业战略方面的工作，称之为“black core”[BCORE]。Black core 中涉及了从基于边界的安全模型转移到关注单个事务安全的模型。】
- 草案 1 中 304 行,【The work of the Jericho Forum publicized the idea of limiting

奇安信身份安全实验室出品

implicit trust based on network location and the limitations of relying on static defenses [JERICHO].】修改为【The work of the Jericho Forum in 1994 publicized the idea of de-perimeterization—limiting implicit trust based on network location and the limitations of relying on single, static defenses over a large network segment [JERICHO].】，即【Jericho 论坛的工作公开了限制基于网络位置赋予隐式信任的思想和依赖静态防御的局限性[Jericho]。】修改为【Jericho 论坛的工作公开了去边界化的思想—限制基于网络位置默认的信任，以及在一张大网上依赖单一的、静态的防御的局限性[JERICHO]】。

- 草案 1 中 307 行，去掉~~(now at Palo Alto Networks).~~
- 草案 1 中 308 行，去掉【~~This work included key concepts and a zero trust network architecture model that improved upon the concepts discussed in the Jericho Forum.~~】，即去掉【~~这项工作包括关键概念和零信任网络架构模型，该模型改进了在 Jericho 论坛上讨论的概念。~~】
- 草案 1 中 309 行，增加【Zero trust then became the term used to describe various cybersecurity solutions that moved security away from implied trust based on network location and instead focused on evaluating trust on a per-transaction basis. Both private industry and higher education have also undergone this evolution from perimeter-based security to a security strategy based on zero trust principles.】即【零信任后来成为一个术语，用来描述各种网络安全解决方案，这些解决方案将安全性从基于网络位置的默认信任转移到基于每个事务的信任评估上来。私人企业和高等教育行业也经历了从基于边界的安全到基于零信任原则的安全战略的演变。】
- 草案 1 中 320 行，增加【to a “need to access” basis to mitigate data exposure due to compromised accounts, attackers monitoring a network, and other threats.】即【“需要访问”为基础，减轻由于帐户受损、攻击者监视网络和其他威胁而导致的数据暴露。】

奇安信身份安全实验室出品

1.1 Structure of This Document

2. Zero Trust Basics

- 草案 1 中 340 行，第二章的标题【Zero Trust Network Architecture】修改为【Zero Trust Basics】。
- 草案 1 中 341 行，增加一句【Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.】即【零信任是一种以资源保护为核心的网络安全范式，其前提是信任从来不是隐式授予的，而是必须进行持续评估。】
- 草案 1 中 341 行,【network/data security】修改为【enterprise resource and data security】，即【网络/数据安全】修改为【企业资源和数据安全】。
- 草案 1 中 342 行,【identity】修改为【identity (person and non-person entities)】对 identity 进行了明确，包括人和非人的实体。
- 草案 1 中 343 行，删除【~~Zero trust is an architectural approach that is focused on data protection.~~】。
- 草案 1 中 344 行，【The initial focus should be on restricting resource access to those with a "need to know.】修改为【The initial focus should be on restricting resources to those with a need to access and grant only the minimum privileges (e.g., read, write, delete) needed to perform the mission.】即将【需要知悉】修改为【需要访问并仅授予执行任务所需的最小权限（如读取、修改、删除）】。
- 草案 1 中 350 行，增加【(the TICs and perimeter firewalls) and cannot protect users outside of the perimeter (e.g., remote workers, cloud-based services).】即【无法保护边界外的用户（例如，远程工作者、基于云的服务）】，表明 TIC（Trusted Internet Connections，可信互联网连接）和边界防火墙在在检测和阻止来自网络内部的攻击方面用处不大并且也无法保护边界外的用户（例如，远程工作者、基于云的服务）。
- 草案 1 中 351 行，在第一版草案的 ZTA 的定义，在第二版中修改为 ZT 和 ZTA 的定

© 2020 奇安信集团 保留所有权利

义。【Zero Trust Architecture (ZTA) provides a collection of concepts, ideas, and component relationships (architectures) designed to eliminate the uncertainty in enforcing accurate access decisions in information systems and services.】修改为【Zero trust (ZT) provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.】即【零信任体系结构（ZTA）提供了一系列概念、思想和组件关系（体系架构），旨在消除在信息系统和服务中实施准确访问决策时的不确定性。】修改为【零信任（Zero trust，ZT）提供了一系列概念和思想，旨在面对被视为受损的网络时，减少在信息系统和服务中执行准确的、按请求访问决策时的不确定性。零信任架构（ZTA）是一种企业网络安全规划，它利用零信任概念，并囊括其组件关系、工作流规划与访问策略。因此，零信任企业作为零信任架构规划的产物，是指为企业准备的（物理和虚拟的）网络基础设施及操作策略。】

- 草案 1 中 355 行，增加一段【An enterprise decides to adopt zero trust as its cybersecurity foundation and generate a zero trust architecture as a plan developed with zero trust principles in mind. This plan is then deployed to produce a zero trust environment for use in the enterprise.】即【一个企业决定采用零信任作为它的网络安全基础，并将零信任架构作为一个以零信任原则开发的计划。然后部署此计划以生成一个零信任环境，供企业使用。】
- 草案 1 中 355 行，【which is to eliminate unauthorized access to data and services】修改为【which is the goal to prevent unauthorized access to data and services】，即【这是为了消除对数据和服务的未经授权的访问】修改为【这是为了防止未经授权访问数据和服务】。

奇安信集团安全研究院出品

- 草案 1 中 357 行，【subjects (user/machine)】修改为【subjects (combination of user, application, and device)】即原本的主体指用户/机器，修改为主体是用户、应用和设备的组合。
- 草案 1 中 362 行，【minimizing temporal delays in ~~network~~ authentication mechanisms.】修改为【minimizing temporal delays in authentication mechanisms.】即【最小化网络认证机制中的时间延迟】修改为【最小化认证机制中的时间延迟】，去掉了网络。
- 草案 1 中 370 行，【trustworthy】修改为【authentic】，即【值得信赖的】修改为【真实的】。
- 草案 1 中 372 行，【Can the system remove sufficient doubt about the user's true identity? Is the user justified in their access request? Is the device used for the request trustworthy?】修改为【What is the level of confidence about the user's identity for this unique request? Is access to the resource allowable given the level of confidence in the user's identity? Does the device used for the request have the proper security posture? Are there other factors that should be considered and that change the confidence level (e.g., time, location of subject, subject's security posture)?】即【系统能消除对用户真实身份的足够怀疑吗？用户的访问请求是否合理？用于请求的设备是否可信？】修改为【对于这个唯一的请求，用户的身份的可信度是多少？考虑到对用户身份的信任程度，是否允许访问资源？用于请求的设备是否具有正确的安全姿态？是否有其他因素需要考虑，这些因素可能改变可信度（如时间、主体位置、主体安全姿态）？】
- 草案 1 中 374 行，【Overall, enterprises need to develop risk-based policies for resource access and set up a system to ensure that these policies are executed correctly.】修改为【Overall, enterprises need to develop and maintain dynamic risk-based policies for resource access and set up a system to ensure that these policies are enforced correctly and consistently.】即【总的来说，企业需要为资源访问制定基于风险的策略，并建立一个系统来确保这些策略的正确执行】修改为【总的来说，企业需要为资源访问制定和维护动态的

奇安信身份安全实验室出品

基于风险的策略，并建立一个系统来确保这些策略得到正确和一致的执行。】

- 草案1中377行，【(i.e., logging into a system)】修改为【(logging into an asset)】，即【登录系统】修改为【登录到资产】。
- 草案1中382行，【all the cleared passengers have a common trust level.】修改为【all the cleared passengers are considered trusted.】即【所有通过检查的乘客都有一个共同的信任级别。】修改为【所有通过检查的乘客都被认为是可信的。】
- 草案1中388行，【“Zero Trust Architecture provides technology and capabilities to allow the PDP/PEPs to move closer to the resource. The idea is to authenticate and authorize every single flow in the network from actor (or application) to data.】修改为【Zero trust provides a set of principles and concepts around moving the PDP/PEPs closer to the resource. The idea is to explicitly authenticate and authorize all users, devices, applications, and workflows that make up the enterprise.】即【零信任体系结构提供了技术和能力，允许PDP/PEP更接近资源。其思想是对网络中从参与者（或应用）到数据的每个流进行身份验证和授权。】修改为【零信任提供了一套原则和概念，使PDP/PEP更接近资源。其思想是明确地验证和授权组成企业的所有用户、设备、应用程序和工作流。】

2.1 Tenets of Zero Trust Architecture

- 草案1中391行，2.1题目修改为【Tenets of Zero Trust】，零信任的宗旨。
- 草案1中394行，增加“as part of the functional capabilities of a ZTA.”，即一些微分段的方案依然将边界防护作为“零信任功能的一部分”。
- 草案1中396行，增加【These tenets are the ideal goal, though it must be acknowledged that not all tenets may be fully implemented in their purest form for a given strategy.】即【这些宗旨是理想目标，尽管必须承认，并非所有的宗旨都可以在给定的战略中以其最纯粹的形式得到充分实现。】
- 草案1中400行，增加“software as a service (SaaS)”。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

- 草案 1 中 409 行，【All communication should be done in a secure manner (i.e., encrypted and authenticated).】修改为【All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.】，即【所有通信应以安全的方式进行（即加密和认证）。】修改为【所有通信应以最安全的方式进行，保护机密性和完整性，并提供源身份认证。】
- 草案 1 中 413 行，【before initiating a connection with a resource." 修改为"before initiating a session or performing a transaction with a resource.】即【在启动与资源的连接之前】修改为【启动会话或使用资源执行事务之前。】
- 草案 1 中 413 行，【authentication】修改为【authentication and authorization】，即变为【认证和授权】。
- 草案 1 中 416 行，【including the observable state of user identity and the requesting system】修改为【including the observable state of client identity, application, and the requesting asset】，即【包括用户身份和请求系统的的可观察状态】修改为【包括客户身份、应用和请求资产的可观察状态】，扩展了影响动态策略的因素。
- 草案 1 中 417 行【who its members are】修改为【who its members are (or ability to authenticate users from a federated community),】即【其成员是谁】修改为【其成员是谁（或对来自联邦的用户进行身份认证的能力）】。
- 草案 1 中 419 行【assigned by the enterprise to that account.】修改为【assigned by the enterprise to that account or artifacts to authenticate automated tasks.】即【由企业分配给该帐户】修改为【由企业分配给该帐户或工件以认证自动化任务】。
- 草案 1 中 421 行，对于请求资产的状态，除软件版本、网络位置等，增加了【time/date of request】。
- 草案 1 中 423 行，【Policy is the set of attributes an organization assigns to a user, data asset, or application.】修改为【Policy is the set of access rules based on attributes that an organization assigns to a user, data asset, or application.】即【策略是组织分配给用户、数据资产或应用的一组属性。】修

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

改为【策略是基于组织分配给用户、数据资产或应用的属性的访问规则集。】对于策略修正了定义。

- 草案 1 中 425 行,【Resource access policies】修改为【Resource access and action permission policies】即【资源访问策略】修改为【资源访问和操作权限策略】。
- 草案 1 中 430 行,增加一句【No device is inherently trusted. Here, “most secure state possible” means that the device is in the most practicable secure state and still performs the actions required for the mission.】修改为【没有设备是天生可信的。这里,“可能的最安全状态”是指设备处于最可行的安全状态,并且仍然执行任务所需的操作。】
- 草案 1 中 430 行,【establish a Continuing Diagnostics and Mitigation (CDM) program to monitor the state of systems and apply patches/fixes as needed】修改为【establish a CDM or similar system to monitor the state of devices and applications and should apply patches/fixes as needed.】即【建立持续诊断和缓解(CDM)计划,以监控系统状态,并根据需要应用补丁/修复程序】修改为【建立一个 CDM 或类似的系统来监控设备和应用的状态,并根据需要应用补丁/修复程序。】说明不限定必须是 CDM 系统。
- 草案 1 中 432 行,【Systems that are discovered to be subverted, vulnerable, and/or non-enterprise-owned may be treated differently】修改为【Devices that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently】即【被发现为被颠覆、易受攻击和/或非企业所有的系统可能会受到不同的对待】修改为【发现被颠覆、具有已知漏洞和/或不受企业管理的设备可能会受到不同的对待】。修订后的描述更为准确,比如,企业自己的设备也不见得完全受企业管理,这些设备是可能非受控的。
- 草案 1 中 434 行,【system】修改为【device】。
- 草案 1 中 435 行,增加【This may also apply to associated devices (e.g., personally owned devices) that may be allowed to access some resources but not others. This, too, requires a robust monitoring and reporting system in place to provide actionable data about the current state of enterprise

奇安信身份安全实验室出品

resources.】即【这也可能适用于允许访问某些资源但不允许访问其他资源的关联设备（例如，个人拥有的设备）。这也需要一个强大的监控和报告系统来提供关于企业资源当前状态的可操作数据。】

- 草案1中436行，【User authentication】修改为【All resource authentication and authorization】即【用户身份认证】修改为【所有资源身份认证和授权】。
- 草案1中437行，【continuously authenticating.】修改为【continually reevaluating trust in ongoing communication.】即【持续认证】修改为【在通信中进行持续信任评估。】
- 草案1中438行，【An enterprise implementing a ZTA strategy has a user provisioning system in place and uses the system to authorize access to resources.】修改为【An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place.】即【实施ZTA战略的企业有一个用户供应系统，并使用该系统授权对资源的访问。】修改为【实现ZTA的企业应该具有身份、凭证和访问管理（ICAM）以及资产管理系统。】
- 草案1中441行【Continuous monitoring and re-authentication occur throughout user interaction】修改为【Continuous monitoring with possible re-authentication and reauthorization occurs throughout user interaction】即【在用户交互过程中，会持续监视和重新认证】修改为【在整个用户交互过程中，会持续监视，可能的重新认证和重新授权。】
- 草案1中443行，对于策略增加了【anomalous user activity detected】即【检测到异常用户活动】。
- 草案1中445行，增加【The enterprise collects as much information as possible about the current state of network infrastructure and communications and uses it to improve its security posture. An enterprise should collect data about network traffic and access requests, which is then used to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects (see Section 3.3.1).】即【企业尽可能收集有关网络基础架构和通信现状的信息，并利用这些信息改善其安全姿态。

© 2020 奇安信集团 保留所有权利

企业应该收集有关网络流量和访问请求的数据，然后使用这些数据来改进策略的创建和实施。此数据还可用于为来自主体的访问请求提供上下文(请参阅第3.3.1节)。】

- 草案1中446行，“network ID”修改为““user identification (ID)”。
- 草案1中448行，删除【~~or some other identification.~~】。
- 草案1中448行，增加【These tenets apply to work done within an organization or in collaboration with one or more partner organizations and not to public or consumer-facing business processes. An organization cannot impose internal policies on external actors (e.g., customers or general internet users).】即【此类宗旨适用于在一个组织内或与一个或多个合作伙伴组织协作完成的工作，而不适用于面向公众或消费者的业务流程。组织不能将内部政策强加给外部参与者（例如，客户或普通互联网用户)】。

2.2 A Zero Trust View of a Network

2.2.1 Assumptions for Enterprise-Owned Network Infrastructure

- 草案1中457行，【The enterprise private network is not trustworthy.】修改为【The entire enterprise private network is not considered an implicit trust zone.】即【企业专网不值得信赖。】修改为【整个企业专网不被视为隐式信任区。】
- 草案1中459行，【in a secure manner】修改为【in the most secure manner available】，即【以安全的方式】修改为【以最安全的方式】。
- 草案1中466行，【 No device is inherently trusted.】修改为【No resource is inherently trusted.】即【没有设备是天生可信的。】修改为【没有资源是天生可信的。】
- 草案1中466行，【Every device must authenticate itself (either to resource or PEP)】修改为【Every asset must have its security posture evaluated via a PEP】即【每个设备都必须对自身进行身份验证(对resource或PEP)】修改为【每

奇安信身份安全实验室出品

个资产都必须通过 PEP 评估其安全姿态】。

- 草案 1 中 469 行，【provide a higher trust score than the same request】修改为【provide a confidence level higher than the same request】即【提供比同一请求更高的信任分数】修改为【提供高于同一请求的信任程度】。

2.2.2 Assumptions for Non-Enterprise-Owned Network Infrastructure

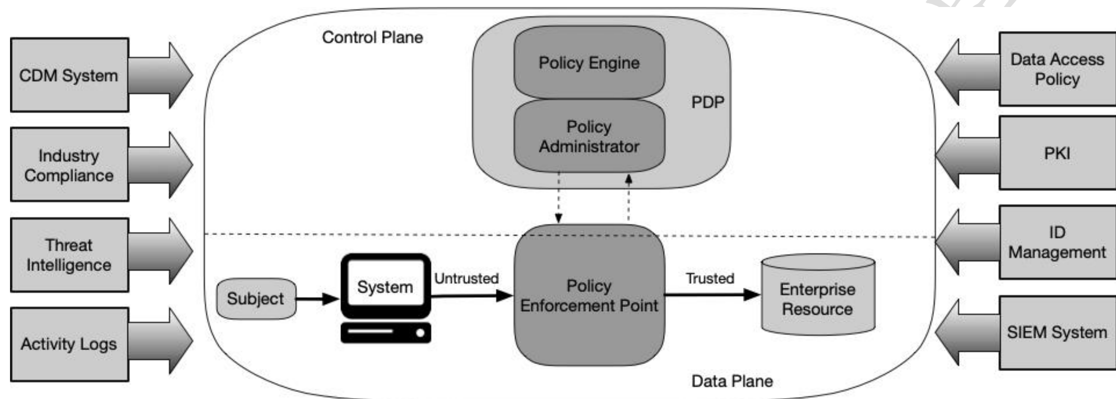
- 草案 1 中 475 行,【The enterprise must be able to monitor, configure, and patch any system, but any system may rely on the local (i.e., non-enterprise) network for basic connectivity and network services (e.g., DNS, etc.).】修改为【Enterprise-owned or -managed assets may need to utilize the local (i.e., nonenterprise) network for basic connectivity and network services (e.g., DNS resolution).】即【企业必须能够监视、配置和修补任何系统，但任何系统都可能依赖本地（即非企业）网络进行基本连接和网络服务（如 DNS 等)】修改为【企业拥有或管理的资产可能需要利用本地（即非企业）网络进行基本连接和网络服务（如 DNS 解析)。】
- 草案 1 中 480 行，【All connection requests should be authenticated, and all traffic should be encrypted】修改为【All connection requests should be authenticated and authorized, and all communications should be done in the most secure manner possible (i.e., provide confidentiality, integrity protection, and source authentication).】即【所有连接请求都应该经过身份认证，所有通信都应该加密】修改为【所有连接请求都应经过身份认证和授权，所有通信都应尽可能以最安全的方式完成（即提供机密性、完整性保护和源身份认证)。】

3. Logical Components of Zero Trust Architecture

- 草案 1 中 485 行，第三章的标题【Zero Trust Architecture Logical Components】修改为【Logical Components of Zero Trust Architecture】。

奇安信集团安全实验室出品

- 草案 1 中 490 行，增加一句【The ZTA logical components use a separate control plane to communicate, while application data is communicated on a data plane (see Section 3.4).】即【ZTA 逻辑组件使用单独的控制平面进行通信，而应用数据在数据平面上进行通信（见第 3.4 节）。】
- 草案 1 中 492 行，针对图 2“零信任核心逻辑组件图”进行了修正，主要包含四处修正：1）policy engine 和 policy administrator 合并称为“PDP”；2）设备明确为 system；3）增加 subject 一项；3）外侧增加一项，Activity logs。



（草案 2 中）零信任核心逻辑组件图

- 草案 1 中 497 行，【grant access to a resource for a given ~~client or~~ subject.】修改为【grant access to a resource for a given subject.】去掉了 client。
- 草案 1 中 498 行，【external sources (e.g., IP blacklists, threat intelligence services)】修改为【external sources (e.g., CDM systems, threat intelligence services described below)】在第三方能力组件中增加了 CDM 系统。
- 草案 1 中 499 行，【to decide to grant or deny access to the resource.】修改为【to grant, deny, or revoke access to the resource.】增加了对访问处理的“”撤销（revoke）”决策。
- 草案 1 中 503 行，【This component is responsible for establishing the connection between a client and a resource.】修改为【This component is responsible for establishing and/or shutting down the communication path between a subject and a resource.】即，增加了 shutting down（关闭），表达更准确；同时连接是在 subject（主体）和 resource（资源）之间的，而不是 client（客户端）和 resource（资源）之间。

© 2020 奇安信集团 保留所有权利

- 草案 1 中 506,【connection（连接)】修改为【session（进程)】。
- 草案 1 中 509,【the connection（连接)】修改为【the communication path（通道)】。
- 草案 1 中 516,【the connection（连接)】修改为【the communication path（通道)】。
- 草案 1 中 516 行，增加【Beyond the PEP is the implicit trust zone (see Section 2) hosting the enterprise resource.】即【在 PEP 之外是托管企业资源的隐式信任区域（请参阅第 2 节)。】
- 草案 1 中 528 行,【(e.g. FISMA, HIPAA, PCI- DSS, etc.).】修改为【e.g., FISMA, healthcare or financial industry information security requirements)】，去掉了 PCI- DSS，使用更为通用的行业安全要求来表达。
- 草案 1 中 530 行，对于 Threat Intelligence Feed(s)，将【This system provides information from outside sources that help the Policy Engine make access decisions.】修改为【This provides information from internal or external sources that help the policy engine make access decisions】即，讲过信息源从外部源，扩展为内部或外部源头；指出威胁情报可能来自于外部也可能来自内部。
- 草案 1 中 533 行,【This also includes DNS blacklists, discovered malware, ~~or command and control systems~~】修改为【This also includes blacklists, newly identified malware, and reported attacks to other assets】，对于【DNS 黑名单】修改为【黑名单】，对于【发现的恶意软件】修改为【新识别的恶意软件】，删除【command and control system】，增加【报告的对其他资产的攻击】。
- 草案 1 中 536 行，数据访问策略,【policies about data access created by the enterprise around enterprise resources.】修改为【policies about access to enterprise resources.】即“关于企业围绕企业资源创建的数据访问的策略。”修改为“有关访问企业资源的策略。”，强调资源层面，而不是数据。
- 草案 1 中 540 行,【These roles and access rules should be based on user roles and the mission needs of the organization.】修改为【These policies should be based on the defined mission roles and needs of the organization.】即

奇安信身份安全实验室出品

【这些角色和访问规则应基于用户角色和组织的任务需求】修改为【这些策略应以本组织确定的任务角色和需要为基础。】

- 草案 1 中 543 行，【actors】修改为【subjects】。
- 草案 1 中 545 行，增加一句【This could also be a PKI that is not built upon X.509 certificates.】即【这也可能是不是建立在 X.509 证书上的 PKI。】
- 草案 1 中 547 行，ID 管理系统，【identity records】修改为【identity records（e.g., lightweight directory access protocol (LDAP) server)】，对身份记录进一步说明为【例如，轻量级目录访问协议（LDAP）服务器】。
- 草案 1 中 550 行，增加【This system may be part of a larger federated community and may include nonenterprise employees or links to nonenterprise assets for collaboration.】即【该系统可能是一个更大的联邦社区的一部分，可能包括非企业员工或链接到非企业资产进行协作。】ID 管理系统，可能会扩展到联邦身份的概念。
- 草案 1 中 551 行，增加一条对于网络和系统活动日志的内容【Network and system activity logs: This is the enterprise system that aggregates asset logs, network traffic, resource access actions, and other events that provide real-time (or near-real-time) feedback on the security posture of enterprise information systems.】即【网络和系统活动日志：这是一个企业系统，它聚合了资产日志、网络流量、资源访问操作和其他事件，这些事件提供关于企业信息系统安全姿态的实时（或接近实时）反馈。】
- 草案 1 中 551 行，修改 SIEM 系统的定义【Security information and event management (SIEM) system: This collects security- centric information for later analysis. This data is then used to refine policies and warn of possible attacks against enterprise assets.】即【安全信息和事件管理（SIEM）系统：它收集以安全为中心的信息以供以后分析。然后，这些数据将用于完善策略并警告可能对企业资产发起的攻击。”】

奇安信集团安全实验室出品

3.1 Variations of Zero Trust Architecture Approaches（新增）

- 新增一节，【3.1 Variations of Zero Trust Architecture Approaches】即【零信任架构方法的变化】。
- 【There are several ways that an enterprise can enact a ZTA for workflows. These approaches vary in the components used and in the main source of policy rules for an organization. Each approach implements all the tenets of ZT (see Section 2.1) but may use one or two (or one component) as the main driver of policies. The approaches include enhanced identity governance - driven, logical micro-segmentation via next-generation firewalls (NGFWs), and network-based segmentation.】即【企业可以通过多种方式为工作流制定 ZTA。这些方法因使用的组件和组织的策略规则的主要来源而异。每种方法都达成了 ZT 的全部宗旨（见第 2.1 节），但可以使用一个或两个（或一个组件）作为策略的主要驱动因素。这些方法包括增强的身份治理驱动、通过下一代防火墙（NGFWs）进行逻辑微分段以及基于网络的分段。】
- 【Certain approaches lend themselves to some use cases more than others. An organization looking to develop a ZTA for its enterprise may find that its chosen use case and existing policies point to one approach over others. That does not mean the other approaches would not work but rather that other approaches may be more difficult to implement and may require more fundamental changes to how the enterprise currently conducts business flows.】即【对于某些用例来说，某些方法会显得比其他方法更适合。为企业研发 ZTA 的组织部门可能会发现，其选择的用例和现有策略指向某一种特定方法而不是其他方法。这并不意味着其他方法不起作用，而是意味着其他方法可能更难实施，并且可能需要对企业当前如何进行业务流造成更根本的更改。】

奇安信身份安全实验室出品

3.1.1 ZTA Using Enhanced Identity Governance

- 标题：使用增强身份治理的 ZTA。
- 【The enhanced identity governance approach to developing a ZTA uses the identity of actors as the key component of policy creation. If it were not for subjects requesting access to enterprise resources, there would be no need to create access polices. For this approach, enterprise resource access policies are based on identity and assigned attributes. The primary requirement for resource access is based on the access privileges granted to the given subject. Other factors such as device used, asset status, and environmental factors may alter the final confidence level calculation (and ultimate access authorization) or tailor the result in some way, such as granting only partial access to a given data source based on network location. Individual resources or PEP components protecting the resource must have a way to forward requests to a policy engine service or authenticate the subject and approve the request before granting access.】即【实现 ZTA 的增强身份治理方法使用参与者身份作为策略创建的关键组件。如果不是针对请求访问企业资源的主体，则无需创建访问策略。对于这种方法，企业资源访问策略基于身份和分配的属性。资源访问的主要要求基于授予给定主体的访问权限。其他因素，如使用的设备、资产状态和环境因素，可以改变最终信任程度算（和最终访问授权），或者以某种方式调整结果，例如基于网络位置仅授予对给定数据源的部分访问。保护资源的单个资源或 PEP 组件必须具有将请求转发到策略引擎服务或认证主体并在授予访问权限之前批准请求的方法。】
- 【Enhanced identity governance-based approaches for enterprises are often found using an open network model or an enterprise network with visitor access or frequent nonenterprise devices on the network (such as with the use case in Section 4.3 below). Network access is initially granted to all assets with access to resources that are restricted to identities with the appropriate access privileges. The identity-driven approach works well with

奇安信身份安全实验室出品

the resource portal model since device identity and status provide secondary support data to access decisions. Other models work as well, depending on policies in place.】即【针对企业的基于增强身份治理的方法通常使用开放网络模型或有访客访问的企业网络或非企业设备常接入网络的情况(如下面第 4.3 节中的用例)。网络访问最初被授予对资源具有访问权限的所有资产，这些资源仅限于具有适当访问权限的身份。身份驱动的方法与资源门户模型很好地配合，因为设备身份和状态为访问决策提供辅助支持数据。其他模式也可以工作，这取决于现有的策略。】

3.1.2 ZTA Using Micro-Segmentation

- 标题：使用微分段的 ZTA。
- 【An enterprise may choose to implement a ZTA based on placing individual or groups of resources on its own network segment protected by a gateway security component. In this approach, the enterprise places NGFWs or gateway devices to act as PEPs protecting each resource or group of resources. These gateway devices dynamically grant access to individual requests from a client asset. Depending on the model, the gateway may be the sole PEP component or part of a multipart PEP consisting of the gateway and client-side agent (see Section 3.2.1).】即【企业可以选择通过将单个或资源组部署在由网关安全组件保护的自身网段上来实现 ZTA。在这种方法中，企业放置 NGFWs 或网关设备作为 PEP 来保护每个资源或资源组。这些网关设备为来自客户端资产的每个请求动态的授予访问权。根据模型的不同，网关可以是唯一的 PEP 组件，也可以是由网关和客户端代理组成的 PEP 的一部分(见第 3.2.1 节)。】
- 【This approach applies to a variety of use cases and deployment models as the protecting device acts as the PEP, with management of said devices acting as the PE/PA component. This approach requires an identity governance program to fully function but relies on the gateway components to act as the PEP that shields resources from unauthorized access and/or discovery.】

奇安信身份安全实验室出品

即【此方法适用于各种用例和部署模型，因为保护设备充当 PEP，而管理所述设备充当 PE/PA 组件。这种方法需要一个身份治理程序来完全发挥作用，但依赖于网关组件作为 PEP，以保护资源免受未经授权的访问和/或发现。】

- 【The key necessity to this approach is that the PEP components are managed and should be able to react and reconfigure as needed to respond to threats or change in the workflow. It is possible to implement some features of a micro-segmented enterprise by using less advanced gateway devices and even stateless firewalls, but the administration cost and difficulty to quickly adapt to changes make this a very poor choice.】即【这种方法的关键必要性在于，PEP 组件是受管理的，并且应该能够根据需要进行响应和重新配置，以响应工作流中的威胁或更改。虽然通过使用不太先进的网关设备甚至无状态防火墙，可以实现微分隔企业的某些功能，但管理成本和快速适应变化的困难使这成为一个非常糟糕的选择。】

3.1.3 ZTA Using Network Infrastructure and Software Defined Perimeters

- 标题：使用网络基础架构和软件定义边界的 ZTA。
- 【The third approach uses the network infrastructure to implement a ZTA. The ZT implementation could be achieved by using an overlay network (i.e., layer 7 but also could be set up lower of the ISO network stack). These approaches are sometimes referred to as software defined perimeter (SDP) approaches and frequently include concepts from SDN [SDNBOOK] and intent-based networking (IBN) [IBNVN]. In this approach, the PA acts as the network controller that sets up and reconfigures the network based on the decisions made by the PE. The clients continue to request access via PEPs, which are managed by the PA component.】即【第三种方法使用网络基础架构来实现 ZTA。ZT 可以通过使用 overlay 网络实现（即，第 7 层，但也可以设置在 ISO 网络堆栈的较低层）来实现。这些方法有时被称为软件定义边界（SDP）方法，通

奇安信身份安全实验室出品

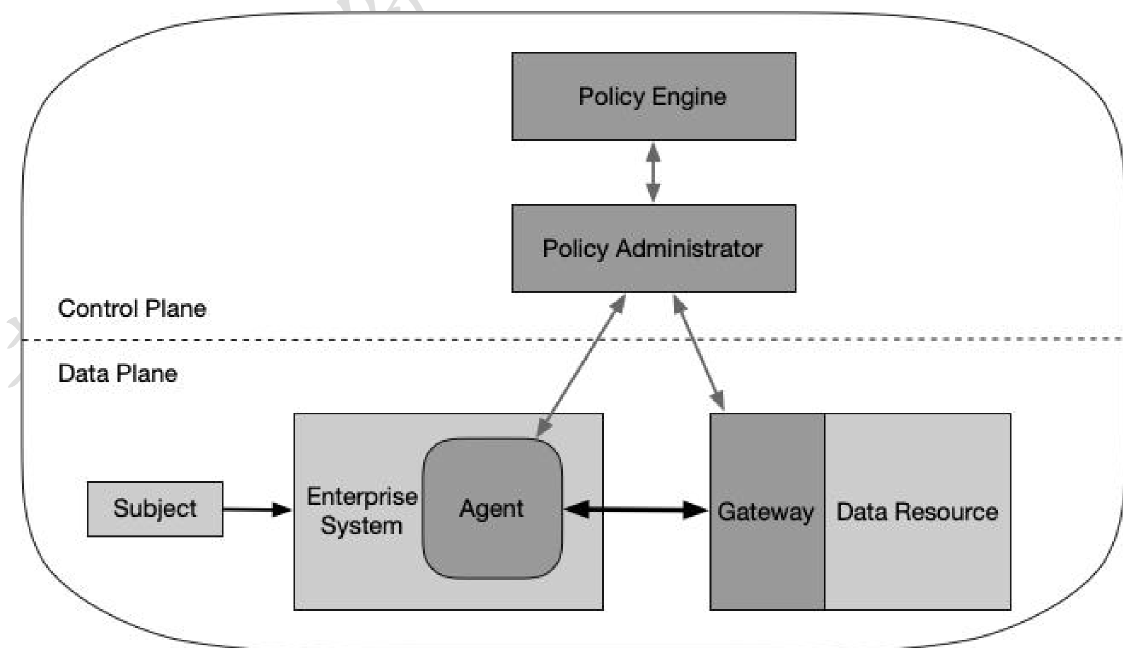
常包括来自 SDN[SDNBOOK]和基于意图的网络(IBN)[IBNVN]的概念。在这种方法中，PA 充当网络控制器，根据 PE 所做的决策建立和重新配置网络。客户端继续通过由 PA 组件管理的 PEPs 请求访问。】

- 【When the approach is implemented at the application network layer (i.e., layer 7), the most common deployment model is the agent/gateway (see Section 3.2.1). In this implementation, the agent and resource gateway (acting as the single PEP and configured by the PA) establish a secure channel used for communication between the client and resource.】即【当该方法在应用网络层（即第 7 层）实现时，最常见的部署模型是代理/网关（见第 3.2.1 节）。在这种实现方法中，代理和资源网关（充当单个 PEP 并由 PA 配置）建立用于客户端和资源之间通信的安全通道。

3.2 Deployed Variations of the Abstract Architecture

3.2.1 Device Agent/Gateway-Based Deployment

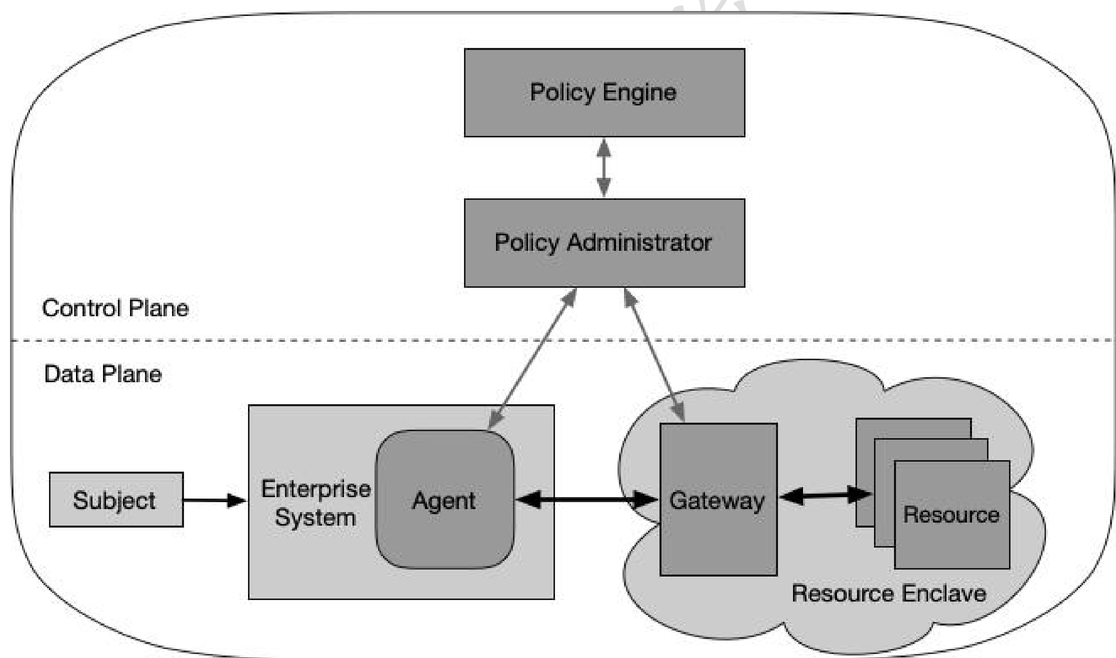
- 对于图 3 进行了修改，增加了 subject 方框。



（草案 2 中）设备代理/网关模型

3.2.2 Enclave-Based Deployment

- 题目从【基于微边界的部署】修改为【Enclave-Based Deployment】即【飞地部署】。
- 草案 1 中 601 行，【(e.g., legacy database system that does not have an API that cannot be used to communicate with a gateway).】修改为【(e.g., legacy database system that does not have an application programming interface [API] that can be used to communicate with a gateway).】即【(例如，传统数据库系没有不能用来与网关通信的 API。)】修改为【例如，传统数据库没有可用于与网关通信的应用程序编程接口[API]。”】
- 草案 1 中图 4，增加了 subject 方框，Gateway 的部署位置作出了修正，和资源一样都在云端。



（草案 2 中）飞地部署模型

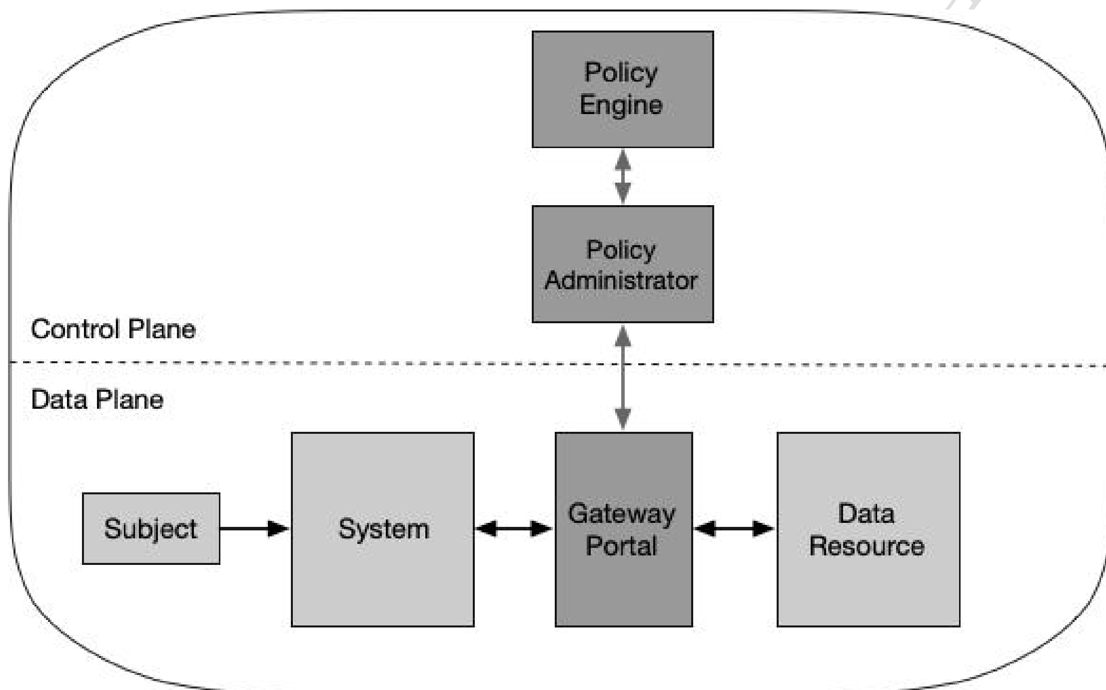
- 草案 1 中 608 行，【microperimeter gateways】，修改为【enclave gateways】，即【微边界网关】修改为【飞地网关】。
- 草案 1 中 611 行，【robust device management program】修改为【robust asset and configuration management program】即【稳健的设备管理程序】修改为【稳健的资产和配置管理计划】。
- 草案 1 中 613 行，删除【“~~This is a relaxation of the ZTA tenet that each resource~~

~~should have its own PEP protecting it.~~】

- 草案 1 中 615 行，“clients”修改为“subject”。

3.2.3 Resource Portal-Based Deployment

- 草案 1 中 618 行，【microperimeter】修改为【a secure enclave】即，【微边界】修改为【安全飞地】。
- 草案 1 中 621 行，图 5 增加主体，subject，enterprise system 修改为 system。



（草案 2 中）资源门户模型

- 草案 1 中 624 行【installed on all enterprise systems.】修改为【installed on all client devices.】即【安装在所有企业系统上】修改为【安装在所有客户端设备上。】
- 草案 1 中 630 行，删除【~~This model allows for more flexibility in client systems and BYOD policies and may make it easier to grant resource access to non-enterprise collaborators.~~】
- 草案 1 中 634 行，增加【The enterprise may be able to employ measures such as browser isolation to mitigate or compensate.】即【企业可以采取浏览器隔离等措施来缓解或补偿。】

© 2020 奇安信集团 保留所有权利

- 草案1中636行,增加【The portal systems should be well-provisioned to provide availability against a DoS attack or network disruption.】即【门户系统应配置好，以提供抵御DoS攻击或网络中断的可用性。】

3.2.4 Device Application Sandboxing

- 题目从【System Application Sandboxing】（系统应用沙箱）修改为【Device Application Sandboxing】（设备应用沙箱）。
- 草案1中638行，【trusted applications】修改为【vetted applications or processes】即【可信应用】修改为【经审查的应用或进程】。
- 草案1中640行，【to protect the application from the host and other applications running on the system.】修改为【to protect the application or instances of applications from a possibly compromised host or other applications running on the asset.】即【以保护应用不受主机和系统上运行的其他应用的影响。】修改为【保护应用或应用实例不受可能受损的主机或资产上运行的其他应用的影响。】
- 草案1中645行,【trusted applications】修改为【approved, vetted applications】,即【可信应用】修改为【批准、审查的应用】。
- 草案1中653行，增加【The enterprise also needs to make sure each sandboxed application is secure, which may require more effort than simply monitoring devices.】即【企业还需要确保每个沙箱应用都是安全的，这可能需要比简单地监视设备需要花费更大精力。】
- 草案1中666行，【The actual request from the application.】修改为【This is the actual request from the subject.】即【来自应用的实际请求。】修改为【来自主体的实际请求】。
- 草案1中668行，【Depending on the system state,】修改为【Depending on these factors and the asset security posture,】即【取决于系统状态】修改为【根据这些因素和资产安全姿态】。
- 草案1中671行，补充参考文献【SP800-63-3】。

© 2020 奇安信集团 保留所有权利

- 草案 1 中 671 行，【enterprise】修改为【enterprise or collaborators】即【企业】修改为【企业或合作者】。
- 草案 1 中 672 行，【user attributes developed by the enterprise】修改为【user attributes/privileges assigned】即【企业开发的用户属性】修改为【已分配用户属性/权限】。
- 草案 1 中 674 行，【logical identity (e.g., account ID/password), biometric data (e.g., fingerprints, facial recognition, iris recognition, retina, and odor/scent), and behavior characteristics (e.g., typing rhythm, gait, and voice).】修改为【logical identity (e.g., account ID) and results of authentication checks performed by PEPs.】即【逻辑身份（如账户 ID/密码）、生物测定数据（如指纹、面部识别、虹膜识别、视网膜和气味/味道）和行为特征（如打字节奏、步态和语音）。】修改为【逻辑身份（如账户标识）和 PEP 执行的认证检查结果。】
- 草案 1 中 677 行，【trust scores】修改为【confidence level】即【信任分】修改为【信任度】。
- 草案 1 中 680 行，增加【This may also include data about past observed user behavior in some (TA) variants (see Section 3.3.1).】即【这也可能包括一些（TA，trust algorithm，信任算法）变化中过去观察到的用户行为的数据（见第 3.3.1 节）】。
- 草案 1 中 684 行，删除“~~Trusted Platform Module (TPM)~~”。
- 草案 1 中 685 行，【Depending on the system state,】修改为【Depending on the asset state compared with this database】即【根据系统状态】修改为【根据资产状态与此数据库进行比较】。
- 草案 1 中 688 行，补充参考文献【SP800-63-3】。
- 草案 1 中 691 行，增加【data sensitivity (sometimes referred to as “data toxicity”)】即【数据敏感性（有时称之为“数据毒性”)】。
- 草案 1 中 695 行，【This can include attack signatures and mitigations.】修改为【These feeds can be external services or internal scans and discoveries and can include attack signatures and mitigations.】即【这可能包括攻击特

奇安信身份安全实验室出品

征和缓解措施】修改为【这些 feed 可以是外部服务，也可以是内部扫描和发现，可以包括攻击签名和缓解措施。】

- 草案 1 中 704 行，增加【PAs may also place a hold or pause on a communication session to reauthenticate and reauthorize the connection in accordance with policy requirements.】即【PA 还可以对通信会话进行保持或暂停，以便根据策略要求重新认证和重新授权连接。】

3.3 Trust Algorithm

3.3.1 Trust Algorithm Variations

- 草案 1 中 710 行，【either as binary decisions or weighted parts of a whole “score.”】修改为【whether as binary decisions or weighted parts of a whole “score” or confidence level.】即【要么是二元决策，要么是整个“分数”的加权部分】修改为【无论是二元决策，还是整体“得分”或信任度的加权部分】。
- 草案 1 中 711 行，【same user (or application) ID.】修改为【same subject, application, or device.】即【相同的用户（或应用）ID】修改为【相同的主体、应用或者设备】。
- 草案 1 中 713 行，【is granted to a resource.】修改为【is granted to a resource or an action (e.g., read/write) is allowed.】即【授予资源】修改为【授予资源或允许操作（例如读/写）】。
- 草案 1 中 714 行，【Access is granted to a resource 】修改为【Access is granted or an action applied to a resource】即【授予对资源的访问权限】修改为【授予访问权限或对资源应用操作】。
- 草案 1 中 715 行，【A score-based TA computes a “score”】修改为【A score-based TA computes a confidence level】，即【基于分数的信任算法计算出一个分数】修改为【基于分数的信任算法计算出一个信任度】。
- 草案 1 中 717 行，【access is granted.】修改为【access is granted, or the action is performed.】即【允许访问】修改为【授予访问权限，或执行操作。】

奇安信身份安全实验室出品

- 草案 1 中 717 行，【Otherwise, the access is denied.】修改为【Otherwise, the request is denied, or access privileges are reduced (e.g., read access is granted but not write access for a file).】即【否则，访问被拒绝。】修改为【否则，请求被拒绝，或访问权限降低（例如，授予读取权限，但不授予对文件的写入权限）。】
- 草案 1 中 726 行，【given user/agent.】修改为【given subject】，即【给定的用户/代理】修改为【给定的主体】。
- 草案 1 中 726 行，增加【Analysis of user behavior can be used to provide a model of acceptable use, and deviations from this behavior could trigger additional authentication checks or resource request denials.】即【用户行为分析可用于提供可接受使用的模型，与此行为的偏差可能会触发额外的身份认证检查或资源请求拒绝。】
- 草案 1 中 727 行，【trust score】修改为【confidence level】。
- 草案 1 中 729 行,【Likewise, a different TA may be score-based but be contextual in that every successful and failed access request could be used to change the ultimate trust score value.】修改为【However, contextual, score-based TAs work best, since the score provides a current confidence level for the requesting account.】即【同样，一个不同的 TA 可以是基于分数的，但必须是上下文的，因为每个成功和失败的访问请求都可以用来更改最终信任分数值。】修改为【但是，基于分数的、上下文的信任算法效果最好，因为分数为请求账户提供了当前的信任度。】
- 草案 1 中 731 行,【this may not always be possible】修改为【this may not always be possible with the infrastructure components available to the enterprise.】即【这并不总是行得通的】修改为【对于企业可用的基础设施组件，这并不总是行得通的。】
- 草案 1 中 739 行，增加【A contextual TA may also send an alert if someone is making access requests after normal business hours】即【如果有人在正常工作时间后提出访问请求，上下文可信算法也可能发送警报】。
- 草案 1 中 751 行，增加【How long this tuning phase lasts depends on the

奇安信身份安全实验室出品

enterprise-defined metrics for progress and tolerance for incorrect access denials/approvals for the resources used in the workflow.】即【此优化阶段持续多长时间取决于企业定义的进度度量和对工作流中使用的资源的错误访问拒绝/批准的容忍度。】

3.4 Network/Environment Components

- 题目从【Network Components】（网络组件）修改为【Network/Environment Components】（网络/环境组件）。
- 草案 1 中 758 行，【infrastructure components】修改为【infrastructure components (both enterprise-owned and from service providers)】即【基础架构组件】修改为【基础架构组件（企业所有和服务提供商提供)】。

3.4.1 Network Requirements to Support ZTA

- 草案 1 中 766 行，【The local network】修改为【The local area network (LAN), enterprise controlled or not】即【局域网】限定为【局域网，无论是否由企业控制】。
- 草案 1 中 769 行，【The enterprise must be able to determine which systems are owned or managed by the enterprise and which devices are not owned or managed.】修改为【The enterprise must be able to distinguish between what assets are owned or managed by the enterprise and their current security posture.】即【企业必须能够确定哪些系统是企业拥有或管理的，哪些设备不是企业拥有或管理的。】修改为【企业必须能够区分企业拥有或管理的资产及其当前的安全姿态。】
- 草案 1 中 771 行，【MAC addresses,】修改为【network MAC addresses that can be spoofed).】即【MAC 地址】修改为【可以伪造的网络 MAC 地址】。
- 草案 1 中 774 行，【but may not be able to perform Deep Packet Inspection (DPI) on all packets.】修改为【but may not be able to perform application layer inspection (i.e., ISO layer 7) on all packets.】即【但可能无法对所有数据包执行深度数据包检查（DPI)】修改为【但可能无法对所有数据包执行应用层检查

© 2020 奇安信集团 保留所有权利

（即，ISO 第 7 层）】。

- 草案 1 中 776 行，增加【to dynamically update policies and inform the PE in evaluating access requests.】即【在评估访问请求时动态更新策略并通知 PE。】
- 草案 1 中 777 行，【discoverable】修改为【reachable】，即【可被发现】修改为【可被访问】。
- 草案 1 中 780 行，增加【Resources may not even be discoverable without accessing a PEP.】即【如果不访问 PEP，资源甚至不可能被发现。】
- 草案 1 中 781 行，【This prevents attackers from scanning the network to identify targets and launching DoS attacks against resources.】修改为【This prevents attackers from identifying targets via scanning and launching DoS attacks against resources located behind PEPs.】即【这可防止攻击者扫描网络以识别目标并对资源发起 DoS 攻击。】修改为【这可防止攻击者通过扫描 PEPs 后面的资源并对其发起 DoS 攻击来识别目标。】
- 草案 1 中 781 行，增加【Note that not all resources should be hidden this way; some network infrastructure components (e.g., DNS servers) must be accessible.】即【请注意，并非所有资源都应以这种方式隐藏；某些网络基础结构组件（如 DNS 服务器）必须可访问】。
- 草案 1 中 784 行，【inaccessible】修改为【not directly accessible】，即【无法访问】修改为【无法直接访问】。
- 草案 1 中 784 行，【Enterprise systems use the data plane when performing network tasks.】修改为【The data plane is used for application data traffic.】即【企业系统在执行网络任务时使用数据平面。】修改为【数据平面用于应用数据通信。】
- 草案 1 中 789 行，【access the PEP component on their enterprise ZTA network in order to gain access to resources.】修改为【access the PEP component to gain access to resources.】即【访问其企业 ZTA 网络上的 PEP 组件以获得对资源的访问】修改为【访问 PEP 组件以访问资源。】
- 草案 1 中 790 行，在 web portal 后补充一个【network device】。
- 草案 1 中 792 行，【The PEP is the only component that can access the Policy

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

Administrator and Policy Engine.】修改为【The PEP is the only component that accesses the policy administrator as part of a business flow.】即【PEP 是唯一可以访问 PA 和策略引擎的组件。】修改为【PEP 是作为业务流的一部分访问 PA 的唯一组件。】

- 草案 1 中 794 行，【The PA may be discoverable, but only PEPs are allowed to connect.】修改为【All enterprise business process traffic passes through one or more PEPs.】即【PA 是可以被发现的，但只有 PEPs 才允许连接。】修改为【所有企业业务流程流量都通过一个或多个 PEP。】
- 草案 1 中 801 行，增加【The infrastructure used to support the ZTA access decision process should be made scalable to account for changes in process load. The PE(s), PA(s), and PEPs used in a ZTA become the key components in any business process. Delay or inability to reach a PEP (or inability of the PEPs to reach the PA/PE) negatively impacts the ability to perform the workflow. An enterprise implementing a ZTA needs to provision the components for the expected workload or be able to rapidly scale the infrastructure to handle increased usage when needed.】即【用于支持 ZTA 访问决策过程的基础架构应具有可扩展性，以考虑过程负载的变化。ZTA 中使用的 PE、PA 和 PEP 成为任何业务流程中的关键组成部分。延迟或无法联系到 PEP（或 PEP 无法联系到 PA/PE）对执行工作流的能力产生负面影响。实现 ZTA 的企业需要为预期的工作负载提供组件，或者能够在需要时快速扩展基础设施以处理增加的使用量。】
- 草案 1 中 802 行，【For example, mobile systems may not be able to reach certain resources unless they are using enterprise network infrastructure.】修改为【For example, there may be a policy stating that mobile assets may not be able to reach certain resources if the requesting asset is located outside of the enterprise’s home country.】即【例如，移动系统可能无法访问到某些资源，除非它们使用企业网络基础设施。】修改为【例如，可能有一项策略规定，如果请求的资产位于企业之外，移动资产可能无法访问到某些资源】。

奇安信集团安全实验室出品

© 2020 奇安信集团 保留所有权利

4. Deployment Scenarios/Use Cases

- 草案 1 中 812 行，【That said, any organization that has a sizable network with multiple resources can benefit from a zero trust architecture.】修改为【That said, any organization can benefit from a zero trust architecture.】即【也就是说，任何拥有具有多个资源的大型网络的组织都可以从零信任结构中获益。】修改为【也就是说，任何组织都可以从零信任结构中获益。】

4.1 Enterprise with Satellite Facilities

- 草案 1 中 827 行，【In this use case, the PE/PA is best hosted as a cloud service with end systems having a connection agent (see Section 3.1.1) or accessing a resource portal (see Section 3.1.3).】修改为【In this use case, the PE/PA(s) is often hosted as a cloud service (which usually provides superior availability and would not require remote workers to rely on enterprise infrastructure to access cloud resources) with end assets having an installed agent (see Section 3.2.1) or accessing a resource portal (see Section 3.2.3).】即【在这个用例中，PE/PA 最好作为一个云服务托管，终端系统有一个连接代理（见第 3.1.1 节）或访问一个资源门户（见第 3.1.3 节)】修改为【在这个用例中，PE/PA 通常作为云服务（通常提供更高的可用性，不需要远程工作者依赖企业基础设施来访问云资源）托管，终端资产具有已安装的代理（见第 3.2.1 节）或访问资源门户（见第 3.2.3 节)。】
- 草案 1 中 830 行，【in order to reach cloud services.】修改为【to reach applications hosted by cloud services.】即【为了达到云服务。】修改为【访问由云服务托管的应用。】

4.2 Multi-Cloud Enterprise

- 草案 1 中 837 行，【Sometimes, the application is hosted on a separate cloud service than the data source.】修改为【Sometimes, the application is hosted

奇安信安全实验室出品

on a cloud service that is separate from the data source.】即【有时，应用托管在一个独立的云服务上，而不是数据源。】修改为【有时，应用托管在与数据源分离的云服务上。】

- 草案 1 中 843 行，删除"~~This multi-cloud use case is one of the main drivers of ZTA adoption.~~ "
- 草案 1 中 848 行，【infrastructure owned by any other service provider.】修改为【infrastructure owned and operated by any other service provider.】即【任何其他服务提供商拥有的基础设施。】修改为【任何其他服务提供商拥有和运营的基础设施。】
- Enterprise with Contracted Services and/or Non-Employee Access
- 草案 1 中 856 行，【and employee work systems.】修改为【and assets.】将【员工工作系统】修改为【资产】。
- 草案 1 中 867 行,【They cannot even conduct network scans to look for enterprise services that may be visible (i.e., prevent active network reconnaissance)】修改为【They may not even be able to discover enterprise services via network scans (i.e., prevent active network reconnaissance/east-west movement).】即【他们甚至不能进行网络扫描以查找可能可见的企业服务（即，阻止主动网络侦察)】修改为【他们甚至可能无法通过网络扫描发现企业服务（即，阻止主动网络侦察/东西移动)。】

4.3 Collaboration Across Enterprise Boundaries

- 草案 1 中 880 行，增加【but this can quickly become difficult to manage. Having both organizations enrolled in a federated ID management system would allow quicker establishment of these relationships provided that both organizations' PEPs can authenticate subjects in a federated ID community.】即【但这很快就会变得难以管理。如果两个组织的 PEP 都可以在联合身份证社区中对主体进行身份认证，那么让两个组织都注册到联合身份证管理系统中可以更快地建立这些关系。】

奇安信身份安全实验室出品

- 草案 1 中 888 行，【Similar to use case 1, the PE and PA would ideally be hosted as a cloud service.】修改为【Similar to Use Case 1, a PE and PA hosted as a cloud service may provide availability to all parties without having to establish a VPN or similar.】即【与用例 1 类似，PE 和 PA 在理想情况下将作为云服务托管。】修改为【与用例 1 类似，作为云服务托管的 PE 和 PA 可以向所有各方提供可用性，而无需建立 VPN 或类似的服务】。

4.4 Enterprise with Public- or Customer-Facing Services（新增）

- 新增一节 4.5，标题为：面向公众或客户提供服务的企业。
- 【A common feature in many enterprises is a public-facing service that may or may not include user registration (i.e., users must create or have been issued a set of login credentials). Such services could be for the general public, a set of customers with an existing business relationship, or a special set of nonenterprise users such as employee dependents. In all cases, it is likely that requesting assets are not enterprise-owned, and the enterprise is constrained as to what internal cybersecurity polices can be enforced. For a general, public-facing resource that does not require login credentials to access (e.g., public web page), the tenets of ZTA do not directly apply. The enterprise cannot strictly control the state of requesting assets, and public resources do not require credentials in order to be accessed. Enterprises may establish policies for registered public users such as customers (i.e., those with a business relationship) and special users (e.g., employee dependents). If the users are required to produce or are issued credentials, the enterprise may institute policies regarding password length, life cycle, and other details and may provide MFA as an option or requirement. However, enterprises are limited in the policies they can implement for this class of user. Information about

奇安信身份安全实验室出品

incoming requests may be useful in determining the state of the public service and detecting possible attacks masquerading as legitimate users. For example, a registered user portal is known to be accessed by registered customers using one of a set of common web browsers. A sudden increase in access requests from unknown browser types or known outdated versions could indicate an automated attack of some kind, and the enterprise could take steps to limit requests from these identified clients. The enterprise should also be aware of any statutes or regulations regarding what information can be collected and recorded about the requesting users and assets.】即【许多企业的一个共同特点是面向公众的服务，可能包括也可能不包括用户注册（即，用户必须创建或已获得一组登录凭据）。这类服务可以面向公众、一组与现有业务关系的客户，或者一组特殊的非企业用户（如员工家属）。在所有情况下，请求的资产很可能不是企业所有的，并且企业在哪些内部网络安全策略可以实施方面受到限制。对于不需要登录凭据才能访问的一般面向公共的资源（例如，公共网页），ZTA 的原则并不直接适用。企业无法严格控制请求资产的状态，公共资源不需要凭据才能访问。企业可以为注册公共用户（如客户（即与企业有业务关系的用户）和特殊用户（如员工家属）制定策略。如果要求用户出示或获得颁发的凭据，企业可以制定有关密码长度、生命周期和其他详细信息的策略，并可以提供 MFA 作为选项或要求。然而，企业在为这类用户实现策略方面受到限制。有关传入请求的信息可能有助于确定公共服务的状态并检测伪装为合法用户的可能攻击。例如，已知注册用户门户由注册客户使用一组通用 web 浏览器中的一个访问。来自未知浏览器类型或已知过时版本的访问请求突然增加可能表示某种自动攻击，企业可以采取措施限制来自这些已标识客户端的请求。企业还应了解有关可收集和记录请求用户和资产的哪些信息的任何法规或条例。】

5. Threats Associated with Zero Trust Architecture

- 草案 1 中 896 行，【However, there are some threat risks unique to ZTA.】修改为【However, some threats have unique features when implementing a ZTA.】

© 2020 奇安信集团 保留所有权利

即【不过，ZTA 有其特有的威胁风险】修改为【然而，在实施 ZTA 时，面临一些特有的威胁】。

5.1 Subversion of ZTA Decision Process

【无修改】

5.2 Denial-of-Service or Network Disruption

- 草案 1 中 910 行，【(i.e., denial-of-service (DoS) attack)】修改为【(i.e., DoS attack or route hijack)】即增加【路由劫持】。
- 草案 1 中 920 行，【There is also the possibility of the hosting provider accidently taking the Policy Administrator offline. Similar to the Amazon S3 outage in February 20174 that prevented access to customers,…】修改为【A hosting provider may also accidentally take a cloud-based PE or PA offline. Cloud services have experienced disruptions in the past, both infrastructure as a service and SaaS.】即【托管提供商也可能意外地使 PA 下线。类似于 1974 年 2 月亚马逊 S3 的中断，它阻止了用户的访问,】修改【托管提供商也可能意外地使基于云的 PE 或 PA 离线。云服务在过去经历过中断，包括基础设施即服务和 SaaS。】
- 草案 1 中 925 行，增加一句【This could happen due to an attack or simply due to unexpected heavy usage.】即【这可能是由于攻击或只是由于意外的大量使用】。

5.3 Stolen Credentials/Insider Threat

- 题目从【Insider Threat】(内部威胁)修改为【Stolen Credentials/Insider Threat】（被盗凭据/内部威胁）。
- 草案 1 中 930 行，【reduce the risk of an insider attack.】修改为【reduce the risk of an attacker gaining broad access via stolen credentials or insider attack. The ZT principle of no implicit trust based on network location means attackers need to compromise an existing account or device to gain a foothold in an enterprise.】即【降低内部攻击的风险】修改【降低攻击者通过被盗凭据

© 2020 奇安信集团 保留所有权利

或内部攻击获得广泛访问权限的风险。ZT 基于网络位置的无隐式信任原则意味着攻击者只能靠破坏某个已有帐户或设备才能在企业中站住脚。】

- 草案 1 中 932 行，增加【This means that accounts with access policies around resources that an attacker is interested in would be the primary targets for attackers.】即【这意味着针对攻击者感兴趣的资源具有访问策略的帐户将成为攻击者的主要目标。】
- 草案 1 中 932 行，【Implementation of MFA for network access may also reduce the risk of access from a compromised account. However, just like traditional enterprises, an attacker with valid credentials (or a malicious insider) may still be able to access resources for which the account has been granted access. For example, an attacker (or compromised employee) who has the credentials and enterprise-owned system of a valid human resources employee may still be able to access an employee database.】修改【Attackers may use phishing, social engineering, or a combination of attacks to obtain credentials of valuable accounts. “Valuable” may mean different things based on the attacker’s motivation. For instance, enterprise administrator accounts may be valuable, but attackers interested in financial gain may consider accounts that have access to financial or payment resources of equal value. Implementation of MFA for network access may reduce the risk of access from a compromised account. However, just like traditional enterprises, an attacker with valid credentials (or a malicious insider) may still be able to access resources for which the account has been granted access. For example, an attacker or compromised employee who has the credentials and enterprise-owned asset of a valid human resources employee may still be able to access an employee database.】即【为网络访问实施 MFA 还可以降低从受损帐户访问的风险。但是，与传统企业一样，具有有效凭据的攻击者（或恶意内部人员）可能仍然能够访问已授予帐户访问权限的资源。例如，具有有效人力资源员工的凭据和企业拥有的系统的攻击者（或受攻击的员工）仍然可以访问员工数据库。】修改为【攻击者可以使用网络钓鱼、社会工程或攻击组合来获取有价值帐户的凭据。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

基于攻击者的动机，“有价值”可能意味着不同的事情。例如，企业管理员帐户可能是有价值的，但对财务收益感兴趣的攻击者可能会考虑访问同等价值的财务或支付资源的帐户。为网络访问实施 MFA 可以降低从受损帐户访问的风险。但是，与传统企业一样，具有有效凭据的攻击者（或恶意内部人员）可能仍然能够访问已授予帐户访问权限的资源。例如，具有有效人力资源员工的凭据和企业拥有的资产的攻击者或受损员工可能仍然能够访问员工数据库。】

- 草案 1 中 939 行，增加一句【If the compromised credentials are not authorized to access a particular resource, they will continue to be denied access to that resource.】即【如果遭破坏的凭据未被授权访问特定资源，则它们将继续被拒绝访问该资源。】
- 草案 1 中 946 行，【may be opaque to network analysis tools.】修改为【may be opaque to traditional layer 3 network analysis tools.】即【可能对网络分析工具不透明】修改为【可能对传统的第 3 层网络分析工具不透明】。

5.4 Visibility on the Network

【无修改】

5.5 Storage of Network Information

- 草案 1 中 961 行，【are being stored for further analysis,】修改为【are being stored for building contextual policies, forensics, or later analysis,】即【正在存储以供进一步分析,】修改为【存储用于构建上下文策略、取证或后期分析】。
- 草案 1 中 966 行，【network】修改为【enterprise】。
- 草案 1 中 972 行，【from designated (or dedicated) administrator accounts.】修改为【only from designated or dedicated administrator accounts】即，【来自指定（或专用）管理员帐户】修改为【仅来自指定或专用管理员帐户】。

奇安信身份安全实验室出品

5.6 Reliance on Proprietary Data Formats

【无修改】

5.7 Use of Non-Person Entities (NPE) in ZTA Administration.

- 草案 1 中 994 行后，增加【The biggest risk when using automated technology for configuration and policy enforcement is the possibility of false positives (innocuous actions mistaken for attacks) and false negatives (attacks mistaken for normal activity). This can be reduced with regular retuning analysis to correct mistaken decisions and improve the decision process.】即【在使用自动化技术进行配置和策略实施时，最大的风险是可能出现假阳性误报(无害操作被误认为是攻击)和假阴性误报(攻击被误认为是正常活动)。这可以通过定期的重新调整分析来减少，以纠正错误的决策并改进决策过程。】

6. Zero Trust Architecture and Possible Interactions with Existing Federal Guidance

- 题目从【Zero Trust Architecture and Existing Federal Guidance】(零信任架构与现有联邦指南）修改为【Zero Trust Architecture and Possible Interactions with Existing Federal Guidance】(零信任架构与现有联邦指南的可能关联)。

6.1 ZTA and NIST Risk Management Framework

- 草案 1 中 1014 行,【but this is disproportionately restrictive in most cases.】修改为【but this is disproportionately restrictive in the majority of cases and inhibits work from being accomplished.】即,【但在大多数情况下，这是过度限制。】修改为【但在大多数情况下，这一点限制性太大，阻碍了工作的完成。】

奇安信身份安全实验室出品

6.2 ZTA and NIST Privacy Framework

- 草案 1 中 1026 行，增加参考文献[NISTPRIV]。
- 草案 1 中 1028 行，增加【This includes personal information used by the enterprise to support ZTA operations and any biometric attributes used in access request evaluations.】即【这包括企业用于支持 ZTA 操作的个人信息以及访问请求评估中使用的任何生物特征属性。】
- 草案 1 中 1029 行，【Part of the core requirements for ZTA is that an enterprise should inspect and log all traffic on its network. This includes decrypting traffic as much as possible to enable inspection.】修改为【Part of the core requirements for ZTA is that an enterprise should inspect and log traffic (or metadata when dealing with encrypted traffic) in its environment.】即，【ZTA 的核心要求之一是，企业应检查并记录其网络上的所有流量。这包括尽可能对通信量进行解密以启用检查。】修改为【ZTA 的核心要求之一是，企业应该检查并记录其环境中的流量（或处理加密流量时的元数据）。】
- 草案 1 中 1033 行，补充参考文献，[NISTIR8062]。

6.3 ZTA and Federal Identity, Credential, and Access Management Architecture (FCIAM)

【无修改】

6.4 ZTA and Trusted Internet Connections 3.0

- 题目从【ZTA and Trusted Internet Connection (TIC)】(ZTA 与 TIC) 修改为【ZTA and Trusted Internet Connections 3.0】(ZTA 与 TIC3.0)

6.5 ZTA and EINSTEIN (NCPS - National Cybersecurity Protection System)

【无修改】

© 2020 奇安信集团 保留所有权利

6.6 ZTA and Continuing Diagnostics and Mitigations (CDM)

- 草案 1 中 1093 行，【to improve federal agency IT security posture.】修改为【to improve federal agency information technology (IT).】即【改善联邦机构 IT 安全姿态】修改为【改进联邦机构信息技术（IT)。】
- 草案 1 中 1106 行，【at rest and in transit】修改为【at rest, in transit, and in use.】
- 草案 1 中 1108 行，【an enterprise must have a complete inventory of both physical and virtual assets.】修改为【an enterprise must have a system to discover and record physical and virtual assets to create a usable inventory.】即【企业必须有完整的物理和虚拟资产库存。】修改为【企业必须有一个系统来发现和记录物理和虚拟资产，以创建可用的库存。】
- 草案 1 中 1114 行，【network】修改为【network (or those accessing resources remotely)】即【网络（或远程访问资源的网络)】。

6.7 ZTA, Cloud Smart, and the Federal Data Strategy

- 草案 1 中 1123 行，【since the users and resources are located outside of the enterprise network perimeter.】修改为【because the users and resources are located outside of the enterprise network perimeter and are likely to see the most benefit in use, scalability, and security】即【由于用户和资源位于企业网络边界之外。】修改为【因为用户和资源位于企业网络边界之外，他们最能体会到在易用性、可扩展性和安全性方面的益处。】

7. Migrating to a Zero Trust Architecture

7.1 Pure Zero Trust Architecture

- 草案 1 中 1146 行，【it is an engineering exercise】修改为【it is an engineering and organizational exercise in】即【这是一项工程练习】修改为【这是一项工

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利

程和组织工作】。

- 草案 1 中 1147 行，增加【This may include additional organizational changes depending on how the enterprise is currently set up and operating.】即【这可能会带来额外的组织变更，具体取决于企业当前的设置和运行方式。】

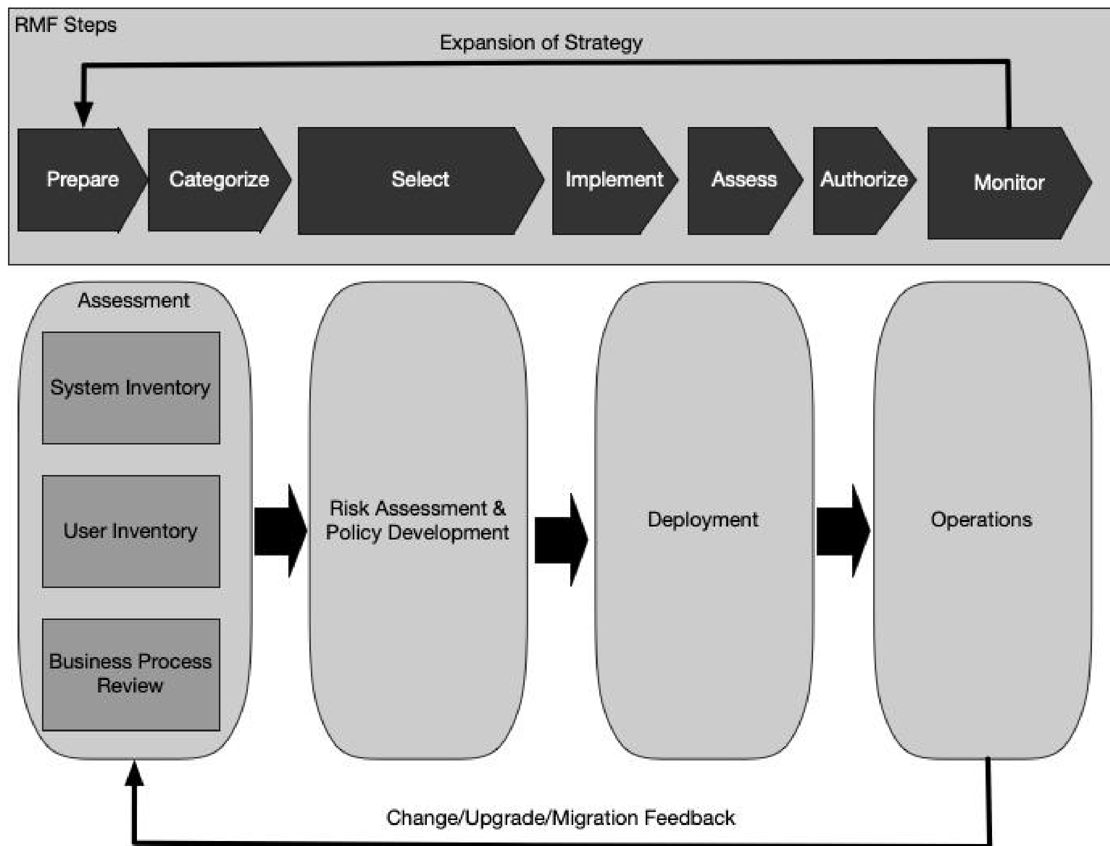
7.2 Hybrid ZTA and Legacy Architecture

7.3 Steps to Introducing ZTA to a Legacy Architected Network

- 草案 1 中 1167 行，【users】修改为【users (including user privileges)】即【用户】修改为【用户（包括用户权限)】。
- 草案 1 中 1169 行，增加【This is especially an issue if there are unknown “shadow IT” deployments operating within an organization.】即【如果组织中有未知的“影子 IT”部署在运行，就明显会成为一个问题。】。
- 草案 1 中 1171 行，【users】后面补充【data flows, and workflows.】，补充【数据流和工作流】。
- 草案 1 中 1176 行，图 12 修改 1）增加了准备阶段；2）RMP steps 增加了反馈箭头（策略的扩展）；3）下面增加了 feedback。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利



（草案 2 中）ZTA 部署周期

7.3.1 Identify Actors on the Enterprise

- 草案 1 中 1187 行，【need additional consideration】修改为【require additional scrutiny】即【需要额外考虑】修改为【要求额外的检查】。
- 草案 1 中 1191 行，【while logging and auditing behavior.】修改为【while using logs and audit actions to identify access behavior patterns.】即【同时记录和审核行为】修改为【同时使用日志和审核操作来标识访问行为模式。】

7.3.2 Identify Assets Owned by the Enterprise

- 草案 1 中 1195 行，【the ability to identify and manage enterprise-owned devices.】修改为【the ability to identify and manage devices.】即【识别和管理企业拥有的设备的能力。】修改为【识别和管理设备的能力。】
- 草案 1 中 1199 行，增加【It may not be possible to conduct a complete census

© 2020 奇安信集团 保留所有权利

on all enterprise-owned assets, so an enterprise should consider building the capability to quickly identify, categorize, and assess newly discovered assets that are on enterprise-owned infrastructure.】即【可能无法对所有企业拥有的资产进行全面的普查，因此企业应考虑建立快速识别、分类和评估企业拥有的基础设施上新发现的资产的能力。】

- 草案 1 中 1207 行，【Non-enterprise-owned assets should also be cataloged to the best extent possible.】修改为【Non-enterprise-owned assets and enterprise-owned "shadow IT" should also be cataloged as well as possible.】即【非企业所有的资产也应尽可能地分类。】修改为【非企业所有资产和企业所有的"影子 IT"也应尽可能分类。】
- 草案 1 中 1201 行，【for monitoring by the enterprise.】修改为【for monitoring and forensics logging by the enterprise.】即【即企业监控】修改为【用于企业监视和取证日志记录】。
- 草案 1 中 1201 行，增加【Shadow IT presents a special problem in that these resources are enterprise-owned but not managed like other resources. Certain ZTA approaches (mainly network-based) may even cause shadow IT components to become unusable as they may not be known and included in network access policies.】即【影子它提出了一个特殊的问题，因为这些资源是企业拥有的，而不是像其他资源一样管理。某些 ZTA 方法（主要是基于网络的方法）甚至可能导致影子 IT 组件变得不可用，因为它们可能不知道并包含在网络访问策略中。】

7.3.3 Identify Key Processes and Evaluate Risks Associated with Executing Process

- 草案 1 中 1221 行,【rank the business processes (i.e., missions) of the agency.】修改为【rank the business processes, data flows, and their relation in the missions of the agency.】即【"对机构的业务流程（即任务）进行排序。】修改为【对机构任务中的业务流程、数据流及其关系进行排序。】
- 草案 1 中 1228 行，增加【and would likely see improvements to availability

and security.】即【而且可能会看到易用性和安全性的改善】。

- 草案 1 中 1228 行，删除~~【This is because the clients and resources are outside of the enterprise perimeter, one of the main advantages of ZTA over legacy enterprise network architecture.”】~~

7.3.4 Formulating Policies for the ZTA Candidate

- 草案 1 中 1240 行，【the next step is to identify the user set that would be affected. ”修改为“identify all upstream resources (e.g., ID management systems, databases, micro-services), downstream resources (e.g., logging, security monitoring), and entities (e.g., users, service accounts) that are used or affected by the workflow.】即【下一步是确定将受影响的用户集】修改为【确定使用或受工作流影响的所有上游资源（如 ID 管理系统、数据库、微服务）、下游资源（如日志记录、安全监控）和实体（如用户、服务帐户）。】

7.3.5 Identifying Candidate Solutions

- 草案 1 中 1262 行，增加【Does the solution provide a means to log interactions for analysis? A key component of ZT is the collection and use of data related to the process flow that feeds back into the PE when making access decisions.】即【该解决方案是否提供了记录交互以进行分析的方法？ZT 的一个关键组成部分是收集和使用与在做出访问决策时反馈到 PE 的过程流相关的数据。】

7.3.6 Initial Deployment and Monitoring

- 草案 1 中 1270 行，【may wish to make them more lenient at first.】修改为【may wish to operate in an observation and monitoring mode at first. 】即【一开始不妨让它们更宽松些。】修改为【可能希望首先以观察和监视模式进行操作。】

奇安信身份安全实验室出品

7.3.7 Expanding the ZTA

- 草案 1 中 1282 行，【After enough confidence is gained in the workflow policy set】修改为【When enough confidence is gained and the workflow policy set is refined】即【在对工作流策略集获得足够的信任之后】修改为【当获得足够的信任并细化工作流策略集时】。
- 草案 1 中 1285 行，增加【The users and stakeholders of the resources and processes involved should also provide feedback to improve operations.】即【相关资源和流程的用户和利益相关者也应提供反馈，以改进运营。】

增加的参考文献：

- [BCORE] 、[FIPS199]、[IBNVN]、[NISTIR 8062]、[NISTPRIV]、[SDNBOOK]、[SP800-63-3]

奇安信身份安全实验室出品

NIST NCCoE 指南《实现零信任架构》（草案）

编者按

为加速对零信任架构的推进工作，在联邦首席信息官（CIO）委员会的要求下，NIST 之前已经发布了《零信任架构》标准草案第 2 版，公开评论目前已经结束。

为配合上述标准的推进工作，2020 年 3 月 NIST 下属单位 NCCoE 发布《实现零信任架构》（草案）项目说明书，征求公开评论。该项目说明书瞄准的是**零信任架构的落地实践**，希望实现**安全性**与**用户体验**的兼得。

我们的观点：作为一项系统工程，安全一点都不简单，不论是传统边界模型，还是零信任模型。零信任的本质是身份与属性管理体系与动态安全策略对 IT 基础设施和应用系统的**深度结合**与**全面覆盖**。在向零信任架构迈进时，请务必夯实安全基础。

1、背景

背景 1：NCCoE 是 NIST 下属单位

2020 年 3 月，国家标准与技术研究所（NIST）下属的 **NCCoE（国家网络安全卓越中心，National Cybersecurity Center of Excellence）**，发布**《实现零信任架构》项目说明书（草案）**，寻求意见反馈。公开评论期现已开放，将于 **2020 年 4 月 14 日结束**。

国家网络安全卓越中心（NCCoE）是 NIST 的一部分，是一个协作中心，在此行业组织、政府机构、学术机构**共同应对企业最紧迫的网络安全挑战**。通过这种合作，NCCoE 开发了模块化、易于调整的**网络安全解决方案示例**，演示如何**使用商用技术**来应用安全标准和最佳实践。

背景 2：联邦首席信息官委员会的努力

近年来，包括 **2015 年人事管理办公室（OPM）数据泄露**在内的几起备受瞩目的网络攻击，都破坏了传统的基于边界的模式。此外，由于云计算的增长、移动性、现代劳动力的变化等因素，边界变得更加模糊和动态。

正是在这种背景下，**联邦首席信息官（CIO）委员会**在 2018 年与 NIST NCCoE 接洽，帮助**联邦机构**围绕 ZTA 的定义达成一致，并了解零信任架构的好处和局限性。联邦机构间的合作，导致了 **NIST SP 800-207《零信任架构》（草案）**的出版。

2019 年 11 月，NCCoE 和联邦 CIO 委员会共同举办了一次**零信任架构技术交流会议**，来自政府和行业的零信任供应商和从业人员聚集一堂，分享在联邦政府和商业部门实施零信任方面的成功经验、最佳做法和经验教训。

NCCoE 项目将建立在这方面的知识基础之上，试图建立并记录一个**与 NIST SP**

© 2020 奇安信集团 保留所有权利

800-207 中的概念和原则相一致并使用商用产品的零信任架构示例。

2、摘要

云计算、移动设备使用、物联网的普及已经模糊了传统的网络边界。企业必须不断发展，为用户提供从**任何位置和设备**对公司资源的安全访问，保护与业务伙伴的交互，保护客户机-服务器以及服务器之间的通信。

零信任的网络安全方法消除了用户和网络的信任假设。它专注于以安全的方式访问资源，而不考虑网络位置、用户和设备，实施严格的访问控制，并不断检查、监视和记录网络流量。这需要数据级的保护、健壮的身份架构、战略性的微分段，以**围绕组织的数字资源创建细粒度信任区**。零信任在开放连接的时间段内，实时评估访问请求和网络流量行为，同时持续不断地重新校准对组织资源的访问。

该 NCCoE 项目将展示一个基于标准的零信任架构的实现。本项目说明书的发布将开始一个过程，该过程将进一步确定项目需求和范围，以及在实验室环境中使用的硬件和软件组件。在实验室中，NCCoE 将构建一个模块化、端到端的**示例零信任架构**，该架构将解决一系列与 NIST 网络安全框架一致的网络安全挑战。该项目将产生一份免费的 **NIST 网络安全实践指南**。

本说明书定义了国家网络安全卓越中心（NCCoE）**项目**，以帮助组织设计零信任。该项目将产生一个 **ZTA 的示例实现，该 ZTA 是根据 NIST SP 800-207 中记录的概念和原则设计和部署的**。更具体地说，**本项目的主要目标是演示一种拟议的网络拓扑结构**，该拓扑结构使得分布在场内和云环境中的不同企业资源(如数据源、计算服务和物联网设备)可以发挥作用，并继承 ZTA 解决方案的特征。

本项目的第二个目标是识别并尽可能减少由于采用具有上述解决方案特征的ZTA策略而对**用户体验**造成的负面影响。一个成功的 ZTA 解决方案应该尽可能少地给用户体验带来不愉快。

该项目将产生一份可公开获取的 **NIST 网络安全实践指南**（NIST Cybersecurity Practice Guide），它是一份详细的实施指南，说明实施网络安全参考设计所需的实际步骤，该设计旨在实现项目目标。

零信任的概念已经存在了十多年，但支持零信任的技术现在才成为主流。零信任架构在很大程度上依赖于用于身份管理、资产管理、应用程序身份验证、网络分段和威胁情报的组件和功能。**零信任架构应该在不牺牲用户体验的情况下增强网络安全**。NCCoE 正在研究零信任及其组件技术的当前行业发展，这些技术支持实用、安全和基于标准的零信任架构的目标。

3、场景

场景 1：员工访问公司资源

奇安信身份安全实验室出品

员工希望从任何工作地点轻松、安全地访问公司资源。此场景将演示一种特定的用户体验，其中员工尝试使用企业管理的设备访问企业服务，如企业内部网、考勤系统和其他人力资源系统。该资源的相关访问请求将由本项目中实现的 ZTA 解决方案动态和实时地提供。

场景 2：员工访问互联网资源

员工正在尝试访问公共 internet 以完成某些任务。此场景将演示一种特定的用户体验，其中员工尝试使用企业管理的设备在 internet 上访问基于 web 的服务。虽然基于 web 的服务不是由企业拥有和管理的，但是该项目中实现的 ZTA 解决方案仍然会动态和实时地提供对该资源的相关访问请求。该解决方案将允许员工在任何位置访问，也就是说，员工可以使用企业管理设备在企业内部网、分支办公室或公共互联网内连接时访问互联网。

场景 3：承包商访问公司和互联网资源

承包商试图访问某些公司资源和互联网。此场景将演示一个特定的用户体验，其中受雇提供特定服务的承包商，试图访问某些公司资源和 internet 以执行组织的计划服务。公司资源可以是本地或云中的，承包商将能够在本地或从公共互联网访问公司资源。承包商试图访问的资源的相关网络访问请求，将由本项目中实施的 ZTA 解决方案动态和实时地提供。

场景 4：企业内的服务器间通信

企业服务通常有不同的服务器相互通信。例如，web 服务器与应用服务器通信。应用服务器与数据库通信以将数据检索回 web 服务器。此场景将演示企业内服务器间交互的示例，其中包括场内、云中或在本地和云中服务器之间的服务器。本项目中实施的 ZTA 解决方案，将动态和实时地提供相互交互的指定服务器之间的关联网络通信。

场景 5：与业务伙伴的跨企业协作

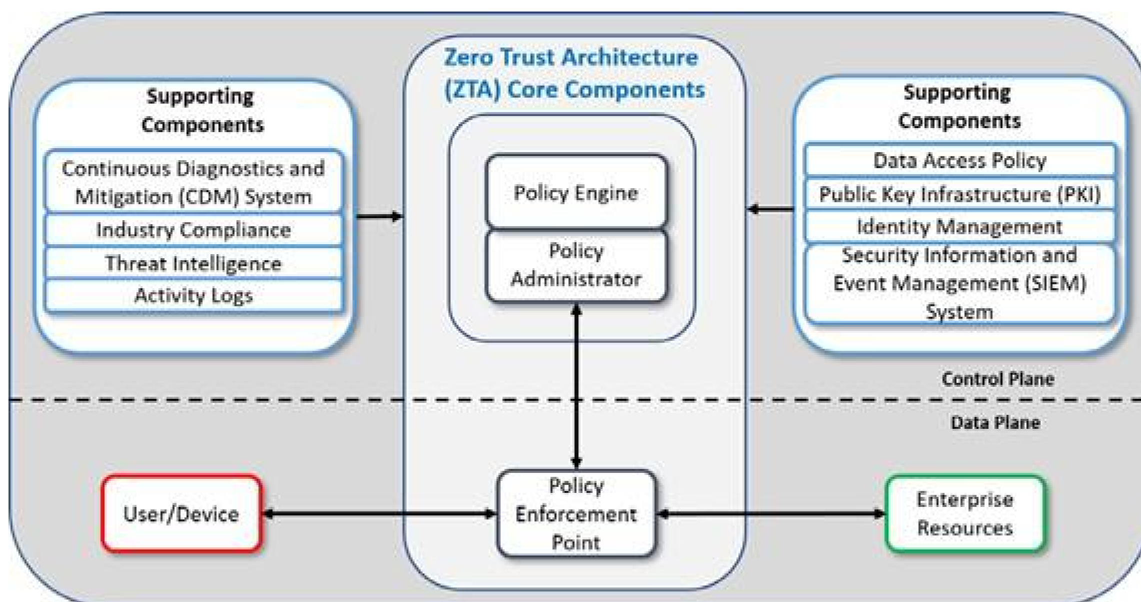
两个企业可以在资源共享的项目上协作。在这种情况下，本项目中实现的 ZTA 解决方案将使一个企业的用户能够安全地访问另一个企业的特定资源，反之亦然。例如，企业 A 用户将能够从企业 B 访问特定的应用程序，而企业 B 用户将能够从企业 A 访问特定的数据库。

场景 6：利用公司资源建立信心水平

企业有监控系统、安全信息和事件管理（SIEM）系统以及其他资源，这些资源可以向策略引擎提供数据，从而为访问企业资源创建更细粒度的信任级别，并促进基于信任级别的严格访问。在这种情况下，ZTA 解决方案将这些监控和 SIEM 系统与策略引擎集成，以生成更精确的置信水平计算。

奇安信身份安全实验室出品

4、架构和组件



ZTA（零信任架构）高层级架构

组件清单

核心组件：策略引擎、策略管理器、策略执行点；

支撑组件：CDM 系统、行业合规系统、威胁情报、网络和访问日志记录系统、数据访问策略、PKI 系统、身份管理系统、SIEM 系统；

设备和网络基础设施组件：设备、网络基础设施组件；

以上组件的定义都直接来自 NIST SP 800-207《零信任架构标准（草案)》，故不再赘述。

期望要求

本项目旨在开发满足以下要求的参考设计和实施：

- 代表了**基于标准的解决方案架构**，该架构是实现 ZTA 的有效和安全方法
- **无需使用第三方工具**（如 VPN、TIC（可信互联网连接)），即可直接访问场内和云中的互联网和公司资源
- 演示与云和企业场内部署资源的集成
- 显示**与标准目录协议和身份管理服务的集成**（例如，轻量级目录访问协议（LDAP)、活动目录（AD)、OpenLDAP、安全断言标记语言（SAML))
- 通过标准 API 演示**与传统和当前的 SIEM 工具的集成**

© 2020 奇安信集团 保留所有权利

- 显示所需的**企业用户设备安全要求**，包括：静态数据保护，对设备漏洞、设备误用、恶意软件执行、数据丢失风险的缓解，恶意活动的感知和响应等。

奇安信身份安全实验室出品

© 2020 奇安信集团 保留所有权利